

RANDOM SUBDICTIONARIES AND COHERENCE CONDITIONS FOR SPARSE SIGNAL RECOVERY

ALEXANDER BARG*, ARYA MAZUMDAR†, AND RONGRONG WANG‡

ABSTRACT. The most frequently used condition for sampling matrices employed in compressive sampling is the restricted isometry (RIP) property of the matrix when restricted to sparse signals. At the same time, imposing this condition makes it difficult to find explicit matrices that support recovery of signals from sketches of the optimal (smallest possible) dimension. A number of attempts have been made to relax or replace the RIP property in sparse recovery algorithms. We focus on the relaxation under which the near-isometry property holds for most rather than for all submatrices of the sampling matrix, known as statistical RIP or StRIP condition. We show that sampling matrices of dimensions $m \times N$ with maximum coherence $\mu = O((k \log^3 N)^{-1/4})$ and mean square coherence $\bar{\mu}^2 = O(1/(k \log N))$ support stable recovery of k -sparse signals using Basis Pursuit. These assumptions are satisfied in many examples. As a result, we are able to construct sampling matrices that support recovery with low error for sparsity k higher than \sqrt{m} , which exceeds the range of parameters of the known classes of RIP matrices.

1. INTRODUCTION

One of the important problems in theory of compressed sampling is construction of sampling operators that support algorithmic procedures of sparse recovery. A universal sufficient condition for stable reconstruction is given by the restricted isometry property (RIP) of sampling matrices [14]. It has been shown that sparse signals compressed to low-dimensional images using linear RIP maps can be reconstructed using ℓ_1 minimization procedures such as Basis Pursuit and Lasso [20, 18, 14, 11],

Let \mathbf{x} be an N -dimensional real signal that has a sparse representation in a suitably chosen basis. We will assume that \mathbf{x} has k nonzero coordinates (it is a k -sparse vector) or is approximately sparse in the sense that it has at most k significant coordinates, i.e., entries of large magnitude compared to the other entries. The observation vector \mathbf{y} is formed as a linear transformation of \mathbf{x} , i.e.,

$$\mathbf{y} = \Phi \mathbf{x} + \mathbf{z},$$

where Φ is an $m \times N$ real matrix, $m \ll N$, and \mathbf{z} is a noise vector. We assume that \mathbf{z} has bounded energy (i.e., $\|\mathbf{z}\|_2 < \varepsilon$). The objective of the estimator is to find a good approximation of the signal \mathbf{x} after observing \mathbf{y} . This is obviously impossible for general signals \mathbf{x} but becomes tractable if we seek a sparse approximation $\hat{\mathbf{x}}$ which satisfies

$$(1) \quad \|\mathbf{x} - \hat{\mathbf{x}}\|_p \leq C_1 \min_{\mathbf{x}' \text{ is } k\text{-sparse}} \|\mathbf{x} - \mathbf{x}'\|_q + C_2 \varepsilon$$

for some $p, q \geq 1$ and constants C_1, C_2 . Note that if \mathbf{x} itself is k -sparse, then (1) implies that the recovery error $\|\hat{\mathbf{x}} - \mathbf{x}\|$ is at most proportional to the norm of the noise. Moreover it implies that the recovery is stable in the sense that if \mathbf{x} is approximately k -sparse then the recovery error is small. If the estimate satisfies an inequality of the type (1), we say that the recovery procedure satisfies a (p, q) error guarantee.

Among the most studied estimators is the Basis Pursuit algorithm [23]. This is an ℓ_1 -minimization algorithm that provides an estimate of the signal through solving a convex programming problem

$$(2) \quad \hat{\mathbf{x}} = \arg \min \|\tilde{\mathbf{x}}\|_1 \quad \text{subject to } \|\Phi \tilde{\mathbf{x}} - \mathbf{y}\|_2 \leq \varepsilon.$$

Basis Pursuit is known to provide both (ℓ_1, ℓ_1) and (ℓ_2, ℓ_1) error guarantees under the conditions on Φ discussed in the next section.

Another popular estimator for which the recovery guarantees are proved using coherence properties of the sampling matrix Φ is Lasso [45, 23]. Assume the vector \mathbf{z} is independent of the signal and formed of independent identically

Date: March 11, 2013.

* Dept. of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742, and Institute for Problems of Information Transmission, Russian Academy of Sciences, Moscow, Russia. Email: abarg@umd.edu. Research supported in part by NSF grants CCF0916919, CCF1217245, CCF1217894, DMS1101697, and NSA H98230-12-1-0260.

† Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139. This work was done while the author was at the University of Maryland, College Park, MD. Email: aryam@mit.edu.

‡ Dept. of Mathematics, University of Maryland, College Park, MD 20742. Email: rwang928@math.umd.edu.

distributed Gaussian random variables with zero mean and variance σ^2 . Lasso is a regularization of the ℓ_0 minimization problem written as follows:

$$(3) \quad \hat{\mathbf{x}} = \arg \min_{\tilde{\mathbf{x}} \in \mathbb{R}^N} \frac{1}{2} \|\Phi \tilde{\mathbf{x}} - \mathbf{y}\|_2^2 + \lambda_N \sigma^2 \|\tilde{\mathbf{x}}\|_{\ell_1}.$$

Here λ_N is a regularization parameter which controls the complexity (sparsity) of the optimizer.

Compressed sensing is just one of a large group of applications of solutions of severely ill-defined problems under the sparsity assumption. An extensive recent overview of such applications is given in [10]. It is this multitude of concrete applications that makes the study of sparse recovery such an appealing area of signal processing and applied statistics.

1.1. Properties of sampling matrices. One of the main questions related to sparse recovery is derivation of sufficient conditions for the convergence and error guarantees of the reconstruction algorithms. Here we discuss some properties of sampling matrices that are relevant to our results, focusing on incoherence and near-isometry of random submatrices of the sampling matrix.

Let Φ be an $m \times N$ real matrix and let ϕ_1, \dots, ϕ_N be its columns. Without loss of generality throughout this paper we assume that the columns are unit-length vectors. Let $[N] = \{1, 2, \dots, N\}$ and let $I = \{i_1, \dots, i_k\} \subset [N]$ be a k -subset of the set of coordinates. By $\mathcal{P}_k(N)$ we denote the set of all k -subsets of $[N]$. Below we write Φ_I to refer to the $m \times k$ submatrix of Φ formed of the columns with indices in I . Given a vector $\mathbf{x} \in \mathbb{R}^N$, we denote by \mathbf{x}_I a k -dimensional vector given by the projection of the vector \mathbf{x} on the coordinates in I .

It is known that at least $m = \Omega(k \log(N/k))$ samples are required for any recovery algorithm with an error guarantee of the form (1) (see for example [36, 37]). Matrices with random Gaussian or Bernoulli entries with high probability provide the best known error guarantees from the sketch dimension that matches this lower bound [20, 21, 19]. The estimates become more conservative once we try to construct sampling matrices explicitly.

We say that Φ satisfies the *coherence property* if the inner product $|\langle \phi_i, \phi_j \rangle|$ is uniformly small, and call $\mu = \max_{i \neq j} |\langle \phi_i, \phi_j \rangle|$ the coherence parameter of the matrix. The importance of incoherent dictionaries has been recognized in a large number of papers on compressed sensing, among them [46, 49, 30, 17, 15, 16, 11]. The coherence condition plays an essential role in proofs of recovery guarantees in these and many other studies. We also define the mean square coherence and the maximum average square coherence of the dictionary:

$$\bar{\mu}^2 = \frac{1}{N(N-1)} \sum_{\substack{i,j=1 \\ i \neq j}}^n \mu_{ij}^2, \quad \bar{\mu}_{\max}^2 = \max_{1 \leq j \leq N} \frac{1}{N-1} \sum_{\substack{i=1 \\ i \neq j}}^n \mu_{ij}^2.$$

Of course, $\bar{\mu}^2 \leq \bar{\mu}_{\max}^2$ with equality if and only if for every j the sum in $\bar{\mu}_{\max}^2$ takes the same value. Our reliance on two coherence parameters of the sampling matrix Φ resembles somewhat the approach in [3, 4]; however, unlike those papers, our results imply recovery guarantees for Basis Pursuit. Our proof methods are also materially different from these works. More details are provided below in this section where we comment on previous results.

1.1.1. The RIP property. The matrix Φ satisfies the RIP property (is (k, δ) -RIP) if

$$(4) \quad (1 - \delta) \|\mathbf{x}\|_2^2 \leq \|\Phi \mathbf{x}\|_2^2 \leq (1 + \delta) \|\mathbf{x}\|_2^2$$

holds for all k -sparse vectors \mathbf{x} , where $\delta \in (0, 1)$ is a parameter. Equivalently, Φ is (k, δ) -RIP if $\|\Phi_I^T \Phi_I - \text{Id}\| \leq \delta$ holds for all $I \in [N]$, $|I| = k$, where $\|\cdot\|$ is the spectral norm and Id is the identity matrix. The RIP property provides a sufficient condition for the solution of (2) to satisfy the error guarantees of Basis Pursuit [20, 18, 14, 11]. In particular, by [14], $(2k, \sqrt{2} - 1)$ -RIP suffices for both (ℓ_1, ℓ_1) and (ℓ_2, ℓ_1) error estimates, while [11] improves this to $(1.75k, \sqrt{2} - 1)$ -RIP.

As is well known (see [46] [26]), coherence and RIP are related: a matrix with coherence parameter μ is $(k, (k - 1)\mu)$ -RIP. This connection has served the starting point in a number of studies on constructing RIP matrices from incoherent dictionaries. To implement this idea one starts with a set of unit vectors ϕ_1, \dots, ϕ_N with maximum coherence μ . In other words, we seek a well-separated collection of lines through the origin in \mathbb{R}^m , or reformulating again, a good packing of the real projective space $\mathbb{R}P^{m-1}$. One way of constructing such packings begins with taking a set \mathcal{C} of binary m -dimensional vectors whose pairwise Hamming distances are concentrated around $m/2$. Call the maximum deviation from $m/2$ the *width* w of the set \mathcal{C} . An incoherent dictionary is obtained by mapping the bits of a small-width code to bipolar signals and normalizing. The resulting coherence and width are related by $w(\mathcal{C}) = \mu m/2$.

One of the first papers to put forward the idea of constructing RIP matrices from binary vectors was the work by DeVore [25]. While [25] did not make a connection to error-correcting codes, a number of later papers pursued both its algorithmic and constructive aspects [6, 12, 13, 24]. Examples of codes with small width are given in [2], where they are studied under the name of small-bias probability spaces. RIP matrices obtained from the constructions in [2] satisfy $m = O(\frac{k \log N}{\log(\log k N)})^2$. Ben-Aroya and Ta-Shma [7] recently improved this to $m = O(\frac{k \log N}{\log k})^{5/4}$ for $(\log N)^{-3/2} \leq \mu \leq (\log N)^{-1/2}$. The advantage of obtaining RIP matrices from binary or spherical codes is low construction complexity: in many instances it is possible to define the matrix using only $O(\log N)$ columns while the remaining columns can be computed as their linear combinations. We also note a result by Bourgain et al. [8] who gave the first (and the only known) construction of RIP matrices with k on the order of $m^{\frac{1}{2}+\epsilon}$ (i.e., greater than $O(\sqrt{m})$). An overview of the state of the art in the construction of RIP matrices is given in a recent paper [5].

At the same time, in practical problems we still need to write out the entire matrix; so constructions of complexity $O(N)$ are an acceptable choice. Under these assumptions, the best tradeoff between m, k and N for RIP-matrices based on codes and coherence is obtained from Gilbert-Varshamov type code constructions: namely, it is possible to construct (k, δ) -RIP matrices with $m = 4(k/\delta)^2 \log N$. At the same time, already [2] observes that the sketch dimension in RIP matrices constructed from binary codes is at least $m = \Theta((k^2 \log N)/\log k)$.

1.1.2. Statistical incoherence properties. The limitations on incoherent dictionaries discussed in the previous section suggest relaxing the RIP condition. An intuitively appealing idea is to require that condition (4) hold for almost all rather than all k -subsets I , replacing RIP with a version of it, in which the near-isometry property holds with high probability with respect to the choice of $I \in \mathcal{P}_k(N)$. Statistical RIP (StRIP) matrices are arguably easier to construct, so they have a potential of supporting provable recovery guarantees from shorter sketches compared to the known constructive schemes relying on RIP.

A few words on notation. Let $[N] := \{1, 2, \dots, N\}$ and let $\mathcal{P}_k(N)$ denote the set of k -subsets of $[N]$. The usual notation for probability \Pr is used to refer a probability measure when there is no ambiguity. At the same time, we use separate notation for some frequently encountered probability spaces. In particular, we use P_{R_k} to denote the uniform probability distribution on $\mathcal{P}_k(N)$. If we need to choose a random k -subset I and a random index in $[N] \setminus I$, we use the notation $P_{R'_k}$. We use P_{R^k} to denote any probability measure on \mathbb{R}^k which assigns equal probability to each of the 2^k orthants (i.e., with uniformly distributed signs).

The following definition is essentially due to Tropp [49, 48], where it is called conditioning of random subdictionaries.

Definition 1. An $m \times N$ matrix Φ satisfies the statistical RIP property (is (k, δ, ϵ) -StRIP) if

$$P_{R_k}(\{I \in \mathcal{P}_k(N) : \|\Phi_I^T \Phi_I - \text{Id}\| \leq \delta\}) \geq 1 - \epsilon.$$

In other words, the inequality

$$(5) \quad (1 - \delta)\|x\|_2^2 \leq \|\Phi_I x\|^2 \leq (1 + \delta)\|x\|_2^2$$

holds for at least a $1 - \epsilon$ proportion of all k -subsets of $[N]$ and for all $x \in \mathbb{R}^k$.

A related but different definition was given later in several papers such as [12, 3, 30] as well as some others. In these works, a matrix is called (k, δ, ϵ) -StRIP if inequality (5) holds for at least $1 - \epsilon$ proportion of k -sparse unit vectors $z \in \mathbb{R}^N$. While several well-known classes of matrices were shown to have this property, it is not sufficient for sparse recovery procedures. Several additional properties as well as specialized recovery procedures that make signal reconstruction possible were investigated in [12].

In this paper we focus on the statistical isometry property as given by Def. 1 and mean this definition whenever we mention StRIP matrices. We note that condition (5) is scalable, so the restriction to unit vectors is not essential.

Definition 2. An $m \times N$ matrix Φ satisfies a statistical incoherence condition (is (k, α, ϵ) -SINC) if

$$(6) \quad P_{R_k}(\{I \in \mathcal{P}_k(N) : \max_{i \notin I} \|\Phi_I^T \phi_i\|_2^2 \leq \alpha\}) \geq 1 - \epsilon.$$

This condition is discussed in [29, 47], and more explicitly in [48]. Following [48], it appears in the proofs of sparse recovery in [15] and below in this paper. A somewhat similar average coherence condition was also introduced in [3, 4]. The reason that (6) is less restrictive than the coherence property is as follows. Collections of unit vectors with small coherence (large separation) cannot be too large so as not to contradict universal bounds on packings of $\mathbb{R}^{P^{m-1}}$. At the same time, for the norm $\|\Phi_I^T \phi_i\|_2$ to be large it is necessary that a given column is close to the majority of the k vectors from the set I , which is easier to rule out.

Nevertheless, the above relaxed conditions are still restrictive enough to rule out many deterministic matrices: the problem is that for almost all supports I we require that $\|\Phi_I \phi_i\|$ be small for all $i \notin I$. We observe that this condition can be further relaxed. Namely, let

$$\mathcal{B}(\Phi) = \{t \in \mathbb{R} : \exists I \in \mathcal{P}_k(N), i \in I^c \text{ such that } \|\Phi_I^T \phi_i\|_2 = t\}$$

be the set of all values taken by the coherence parameter. Let us introduce the following definition.

Definition 3. An $m \times N$ matrix Φ is said to satisfy a weak statistical incoherence condition (to be a $(k, \delta, \alpha, \epsilon)$ -WSINC) if

$$(7) \quad \sum_{t \in \mathcal{B}(\Phi)} P_{R'_k}(\{(I, i), I \in \mathcal{A}_\alpha(\Phi), i \in I^c \text{ such that } \|\Phi_I^T \phi_i\|_2 = t\}) g(\delta, t) \leq \frac{\epsilon}{N - k},$$

where $g(\delta, t)$ is a positive increasing function of t and

$$\mathcal{A}_\alpha(\Phi) = \{I \in \mathcal{P}_k(N) : \exists i \in I^c \text{ such that } \|\Phi_I^T \phi_i\|_2^2 > \alpha\}.$$

We note that this definition is informative if $g(\delta, t) \leq 1$; otherwise, replacing it with 1 we get back the SINC condition. Below we use $g(\delta, t) = \exp(-(1 - \delta)^2/(8t^2))$. This definition takes account of the distribution of values of the quantity $\|\Phi_I^T \phi_i\|$ for different choices of the support and a column ϕ_i outside it. For binary dictionaries, the WSINC property relies on a distribution of sums of Hamming distances between a column and a collection of k columns, taken with weights that decrease as the sum increases.

Definition 4. We say that a signal $x \in \mathbb{R}^N$ is drawn from a generic random signal model S_k if

- 1) The locations of the k coordinates of x with largest magnitudes are chosen among all k -subsets $I \subset [N]$ with a uniform distribution;
- 2) Conditional on I , the signs of the coordinates $x_i, i \in I$ are i.i.d. uniform Bernoulli random variables taking values in the set $\{1, -1\}$.

Using previous defined notation, the probability induced by the generic model P_{S_k} can be decomposed as $P_{R_k \times R^k}$.

1.2. Contributions of this paper. Our results are as follows. First, we show that a combination of the StRIP and SINC conditions suffices for stable recovery of sparse signals. In their large part, these results are due to [49]. We incorporate some additional elements such as stability analysis of Basis Pursuit based on these assumptions and give the explicit values of the constants involved in the assumptions. We also show that the WSINC condition together with StRIP is sufficient for bounding the off-support error of Basis Pursuit.

One of the main results of [49, 48] is a sufficient condition for a matrix to act nearly isometrically on most sparse vectors. Namely, an $m \times N$ matrix Φ is $(k, \delta, \epsilon = k^{-s})$ -StRIP if

$$\sqrt{s\mu^2 k \log(k+1)} + \frac{k}{N} \|\Phi\|^2 \leq c\delta,$$

where $s \geq 1$ and c is a constant; see [49], Theorem B. For this condition to be applicable, one needs that $\mu = O(1/\sqrt{k \log(1/\epsilon)})$. For sampling matrices that satisfy this condition, we obtain a near-optimal relation $m = O(k \log(N/\epsilon))$ between the parameters. Some examples of this kind are given below in Sect. 5. As one of our main results, we extend the region of parameters that suffice for (k, δ, ϵ) -StRIP. Namely, in Theorem 4.7 we prove that it is enough to have the relation $\mu = O(1/\sqrt[4]{k \log k \log^3(1/\epsilon)})$. This improvement comes at the expense of an additional requirement on $\bar{\mu}^2 = O(1/(k \log(1/\epsilon)))$ (or a similar inequality for $\bar{\mu}_{\max}^2$), but this is easily satisfied in a large class of examples, discussed below in the paper. These examples in conjunction with Theorem 4.1 and the results in Section 2 establish provable error guarantees for some new classes of sampling matrices.

We note a group of papers by Bajwa and Calderbank [3, 4, 13] which is centered around the analysis of a threshold decoding procedure (OST) defined in [3]. The sufficient conditions in these works are formulated in terms of μ and maximum average coherence $\nu = \frac{1}{N-1} \max_{1 \leq j \leq N} |\sum_{i \neq j} \langle \phi_i, \phi_j \rangle|$. Reliance on two coherence parameters of Φ for establishing sufficient conditions for error estimates in [3] is a shared feature of these papers and our research. At the same time, the OST procedure relies on additional assumptions such as minimum-to-average ratio of signal components bounded away from zero (in experiments, OST is efficient for uniform-looking signals, and is less so for sparse signals with occasional small components). Some other similar assumptions are required for the proofs of the noisy version of OST [4].

We note that there is a number of other studies that establish sufficient conditions for sampling matrices to provide bounded-error approximations in sparse recovery procedures, e.g., [16, 34, 35]. At the same time, these conditions are formulated in terms different from our assumptions, so no immediate comparison can be made with our results.

As a side result, we also calculate the parameters for the StRIP and SINC conditions that suffice to derive an error estimate for sparse recovery using Lasso. This result is implicit in the work of Candés and Plan [15], which also uses the SINC property of sampling matrices. The condition on sparsity for Lasso is in the form $k = O(N/\|\Phi\|^2 \log N)$, so if $\|\Phi\|^2 \approx N/m$, this yields $k \leq O(m/\log N)$. This range of parameters exceeds the range in which Basis Pursuit is shown to have good error guarantees, even with the improvement obtained in our paper. At the same time, both [15] and our calculations find error estimates in the form of bounds on $\|\Phi\mathbf{x} - \Phi\hat{\mathbf{x}}\|_2$ rather than $\|\mathbf{x} - \hat{\mathbf{x}}\|_2$, i.e., on the compressed version of the recovered signal.

In the final section of the paper we collect examples of incoherent dictionaries that satisfy our sufficient conditions for approximate recovery using Basis Pursuit. Two new examples with nearly optimal parameters that emerge are the Delsarte-Goethals dictionaries [39] and deterministic sub-Fourier dictionaries [31]. For instance, in the Delsarte-Goethals case we obtain the sketch dimension m on the order of $k \log^3 \frac{N}{\epsilon}$, which is near-optimal, and is in line with the comments made above.

We also show that the restricted independence property of the dictionary suffices to establish the StRIP condition. Using sets of binary vectors known as orthogonal arrays, we find (k, δ, ϵ) -StRIP dictionaries with $k = O(m^{3/7})$. At the same time, we are not able to show that restricted independence gives rise to the SINC property with good parameter estimates, so this result has no consequences for linear programming decoders.

Acknowledgment: We are grateful to Waheed Bajwa for useful feedback on an early version of this work.

2. STATISTICAL INCOHERENCE PROPERTIES AND BASIS PURSUIT

In this section we prove approximation error bounds for recovery by Basis Pursuit from linear sketches obtained using deterministic matrices with the StRIP and SINC properties.

2.1. StRIP Matrices with incoherence property. It was proved in [49] that random sparse signals sampled using matrices with the StRIP property can be recovered with high probability from low-dimensional sketches using linear programming. In this section we prove a similar result that in addition incorporates stability analysis.

Theorem 2.1. *Suppose that \mathbf{x} is a generic random signal from the model S_k . Let $\mathbf{y} = \Phi\mathbf{x}$ and let $\hat{\mathbf{x}}$ be the approximation of \mathbf{x} by the Basis Pursuit algorithm. Let I be the set of k largest coordinates of \mathbf{x} . If*

- (1) Φ is (k, δ, ϵ) -StRIP;
- (2) Φ is $(k, \frac{(1-\delta)^2}{8 \log(2N/\epsilon)}, \epsilon)$ -SINC,

then with probability at least $1 - 3\epsilon$

$$\|\mathbf{x}_I - \hat{\mathbf{x}}_I\|_2 \leq \frac{1}{2\sqrt{2 \log(2N/\epsilon)}} \min_{\mathbf{x}' \text{ is } k\text{-sparse}} \|\mathbf{x} - \mathbf{x}'\|_1$$

and

$$\|\mathbf{x}_{I^c} - \hat{\mathbf{x}}_{I^c}\|_1 \leq 4 \min_{\mathbf{x}' \text{ is } k\text{-sparse}} \|\mathbf{x} - \mathbf{x}'\|_1$$

This theorem implies that if the signal \mathbf{x} itself is k -sparse then the basis pursuit algorithm will recover it exactly. Otherwise, its output $\hat{\mathbf{x}}$ will be a tight sparse approximation of \mathbf{x} .

Theorem 2.1 will follow from the next three lemmas. Some of the ideas involved in their proofs are close to the techniques used in [21]. Let $\mathbf{h} = \mathbf{x} - \hat{\mathbf{x}}$ be the error in recovery of basis pursuit. In the following $I \subset [N]$ refers to the support of the k largest coordinates of \mathbf{x} .

Lemma 2.2. *Let $s = 8 \log(2N/\epsilon)$. Suppose that $\|(\Phi_I^T \Phi_I)^{-1}\| \leq \frac{1}{1-\delta}$ and*

$$\|\Phi_I^T \phi_i\|_2^2 \leq s^{-1}(1-\delta)^2 \quad \text{for all } i \in I^c := [N] \setminus I.$$

Then

$$\|\mathbf{h}_I\|_2 \leq s^{-1/2} \|\mathbf{h}_{I^c}\|_1.$$

Proof. Clearly, $\Phi \mathbf{h} = \Phi \hat{\mathbf{x}} - \Phi \mathbf{x} = 0$, so $\Phi_I \mathbf{h}_I = -\Phi_{I^c} \mathbf{h}_{I^c}$ and

$$\mathbf{h}_I = -(\Phi_I^T \Phi_I)^{-1} \Phi_I^T \Phi_{I^c} \mathbf{h}_{I^c}.$$

We obtain

$$\begin{aligned} \|\mathbf{h}_I\|_2 &\leq \|(\Phi_I^T \Phi_I)^{-1}\| \|\Phi_I^T \Phi_{I^c} \mathbf{h}_{I^c}\|_2 \leq \frac{1}{1-\delta} \sum_{i \in I^c} \|\Phi_I^T \phi_i\|_2 |h_i| \\ &\leq s^{-1/2} \|\mathbf{h}_{I^c}\|_1, \end{aligned}$$

as required. ■

Next we show that the error outside I cannot be large. Below $\text{sgn}(\mathbf{u})$ is a ± 1 -vector of signs of the argument vector \mathbf{u} .

Lemma 2.3. *Suppose that there exists a vector $\mathbf{v} \in \mathbb{R}^N$ such that*

- (i) *\mathbf{v} is contained in the row space of Φ , say $\mathbf{v} = \Phi^T \mathbf{w}$;*
- (ii) *$\mathbf{v}_I = \text{sgn}(\mathbf{x}_I)$;*
- (iii) *$\|\mathbf{v}_{I^c}\|_{\ell_\infty} \leq 1/2$.*

Then

$$(8) \quad \|\mathbf{h}_{I^c}\|_1 \leq 4\|\mathbf{x}_{I^c}\|_1.$$

Proof. By (2) we have

$$\begin{aligned} \|\mathbf{x}\|_1 &\geq \|\hat{\mathbf{x}}\|_1 = \|\mathbf{x} + \mathbf{h}\|_1 = \|\mathbf{x}_I + \mathbf{h}_I\|_1 + \|\mathbf{x}_{I^c} + \mathbf{h}_{I^c}\|_1 \\ &\geq \|\mathbf{x}_I\|_1 + \langle \text{sgn}(\mathbf{x}_I), \mathbf{h}_I \rangle + \|\mathbf{h}_{I^c}\|_1 - \|\mathbf{x}_{I^c}\|_1. \end{aligned}$$

Here we have used the inequality $\|\mathbf{a} + \mathbf{b}\|_1 \geq \|\mathbf{a}\|_1 + \langle \text{sgn}(\mathbf{a}), \mathbf{b} \rangle$ valid for any two vectors $\mathbf{a}, \mathbf{b} \in \mathbb{R}^N$ and the triangle inequality. From this we obtain

$$\|\mathbf{h}_{I^c}\|_1 \leq |\langle \text{sgn}(\mathbf{x}_I), \mathbf{h}_I \rangle| + 2\|\mathbf{x}_{I^c}\|_1.$$

Further, using the properties of \mathbf{v} , we have

$$\begin{aligned} |\langle \text{sgn}(\mathbf{x}_I), \mathbf{h}_I \rangle| &= |\langle \mathbf{v}_I, \mathbf{h}_I \rangle| \\ &= |\langle \mathbf{v}, \mathbf{h} \rangle - \langle \mathbf{v}_{I^c}, \mathbf{h}_{I^c} \rangle| \\ &\leq |\langle \Phi^T \mathbf{w}, \mathbf{h} \rangle| + |\langle \mathbf{v}_{I^c}, \mathbf{h}_{I^c} \rangle| \\ &\leq |\langle \mathbf{w}, \Phi \mathbf{h} \rangle| + \|\mathbf{v}_{I^c}\|_{\ell_\infty} \|\mathbf{h}_{I^c}\|_1 \\ &\leq \frac{1}{2} \|\mathbf{h}_{I^c}\|_1. \end{aligned}$$

The statement of the lemma is now evident. ■

Now we prove that such a vector \mathbf{v} as defined in the last lemma indeed exists.

Lemma 2.4. *Let \mathbf{x} be a generic random signal from the model \mathcal{S}_k . Suppose that the support I of the k largest coordinates of \mathbf{x} is fixed. Under the assumptions of Lemma 2.2 the vector*

$$\mathbf{v} = \Phi^T \Phi_I (\Phi_I^T \Phi_I)^{-1} \text{sgn}(\mathbf{x}_I)$$

satisfies (i)-(iii) of Lemma 2.3 with probability at least $1 - \epsilon$.

Proof. From the definition of \mathbf{v} it is clear that it belongs to the row-space of Φ and $\mathbf{v}_I = \text{sgn}(\mathbf{x}_I)$. We have $v_i = \phi_i^T \Phi_I (\Phi_I^T \Phi_I)^{-1} \text{sgn}(\mathbf{x}_I) = \langle \mathbf{s}_i, \text{sgn}(\mathbf{x}_I) \rangle$, where

$$\mathbf{s}_i = (\Phi_I^T \Phi_I)^{-1} \Phi_I^T \phi_i \in \mathbb{R}^k.$$

We will show that $|v_i| \leq \frac{1}{2}$ for all $i \in I^c$ with probability $1 - \epsilon$.

Since the coordinates of $\text{sgn}(\mathbf{x}_I)$ are i.i.d. uniform random variables taking values in the set $\{\pm 1\}$, we can use Hoeffding's inequality to claim that

$$(9) \quad P_{R^k}(|v_i| > 1/2) \leq 2 \exp\left(-\frac{1}{8\|\mathbf{s}\|_2^2}\right).$$

On the other hand, for all $i \in I^c$,

$$\begin{aligned}
 \|s_i\|_2 &= \|(\Phi_I^T \Phi_I)^{-1} \Phi_I^T \phi_i\|_2 \\
 &\leq \|(\Phi_I^T \Phi_I)^{-1}\| \|\Phi_I^T \phi_i\|_2 \\
 &\leq \frac{1}{1-\delta} \frac{1-\delta}{\sqrt{8 \log(2N/\epsilon)}} \\
 (10) \qquad &= \frac{1}{\sqrt{8 \log(2N/\epsilon)}}.
 \end{aligned}$$

Equations (9) and (10) together imply for any $i \in I^c$,

$$P_{R^k} \left(|v_i| > \frac{1}{2} \right) \leq 2 \exp \left(- \frac{1}{8(1/\sqrt{8 \log(2N/\epsilon)})^2} \right) = \frac{\epsilon}{N}.$$

Using the union bound, we now obtain the following relation:

$$(11) \qquad P_{R^k} \left(\|v_{I^c}\|_\infty > 1/2 \right) \leq \epsilon.$$

Hence $|v_i| \leq \frac{1}{2}$ for all $i \in I^c$ with probability at least $1 - \epsilon$. ■

Now we are ready to prove Theorem 2.1.

Proof of Theorem 2.1. The matrix Φ is (k, δ, ϵ) -SRIP. Hence, with probability at least $1 - \epsilon$, $\|(\Phi_I^T \Phi_I)^{-1}\| \leq \frac{1}{1-\delta}$. At the same time, from the SINC assumption we have, with probability at least $1 - \epsilon$ over the choice of I ,

$$\|\Phi_I^T \phi_i\|_2^2 \leq \frac{(1-\delta)^2}{8 \log(2N/\epsilon)},$$

for all $i \in I^c$. Thus, Φ_I will have these two properties with probability at least $1 - 2\epsilon$. Then from Lemma 2.2 we obtain that

$$\|h_I\|_2 \leq \frac{1}{\sqrt{8 \log(2N/\epsilon)}} \|h_{I^c}\|_1,$$

with probability $\geq 1 - 2\epsilon$. Furthermore, from Lemmas 2.3, 2.4

$$\|h_{I^c}\|_1 \leq 4 \|x_{I^c}\|_1,$$

with probability $1 - \epsilon$. This completes the proof. ■

2.2. StRIP Matrices with weak incoherence property. In this section we establish a recovery guarantee of Basis Pursuit under the weak SINC condition defined earlier in the paper.

Theorem 2.5. *Suppose that the sampling matrix Φ is (k, δ, ϵ) -StRIP and $(k, \delta, \alpha, \epsilon^2)$ -WSINC, where $\alpha = (1 - \delta)^2 / 8 \log(2N/\epsilon)$ and $g_\delta(t) = \exp(-(1 - \delta)^2 / 8t^2)$. Suppose that the signal x is chosen from the generic random signal model and let \hat{x} be the approximation of x found by Basis Pursuit. Then with probability at least $1 - 4\epsilon$ we have*

$$\|x_{I^c} - \hat{x}_{I^c}\|_1 \leq 4 \min_{x' \text{ is } k\text{-sparse}} \|x - x'\|_1.$$

If x is k -sparse and satisfies the condition $y = \Phi x$, then this theorem asserts that Basis Pursuit will find the support of x . If in addition x is the only k -sparse solution to $y = \Phi x$, then we have $\hat{x} = x$. Note that the WSINC property is not sufficient for the (ℓ_2, ℓ_1) error guarantee. However, once the corrected support is detected, the signal x can be found by solving the overcomplete system $y = \Phi_I x$.

To prove Theorem 2.5, we refine the ideas used to establish Lemma 2.4.

Lemma 2.6. *Suppose that the sampling matrix Φ satisfies the conditions of Theorem 2.5. For any $x \in \mathbb{R}^k$ and $I \subset [N]$ define $v(x, I) = \Phi^T \Phi_I (\Phi_I^T \Phi_I)^{-1} \text{sgn}(x)$. Let*

$$p(I) = P_{R^k}(\|v_{I^c}(x, I)\|_\infty > 1/2),$$

Then

$$P_{R^k}(\{I : p(I) > \epsilon\}) < 3\epsilon.$$

Proof. As in the proof of Lemma 2.4, we define the vector

$$\mathbf{s}_i(I) = (\Phi_I^T \Phi_I)^{-1} \Phi_I^T \phi_i \in \mathbb{R}^k$$

and let $v_i(\mathbf{x}, I)$ be the i th coordinate of the vector $v(\mathbf{x}, I)$. From now on we write simply v_i, \mathbf{s}_i , omitting the dependence on I and \mathbf{x} . Let $M = M(\Phi) := \{I \in \mathcal{P}_k(N) : \|\Phi_I^T \Phi_I\|_2 \geq 1 - \delta\}$, then the StRIP property of Φ implies that

$$P_{R_k}(M) \geq 1 - \epsilon.$$

By definition, for any $I \in M$

$$\|\mathbf{s}_i\|_2 = \|(\Phi_I^T \Phi_I)^{-1} \Phi_I^T \phi_i\|_2 \leq \frac{1}{1 - \delta} \|\Phi_I^T \phi_i\|_2.$$

Now we split the target probability into three parts:

$$\begin{aligned} P_{R_k}(\{I : p(I) > \epsilon\}) &= P_{R_k}(\{I \in M \cap A : p(I) > \epsilon\}) + P_{R_k}(\{I \in M \cap A^c : p(I) > \epsilon\}) \\ &\quad + P_{R_k}(\{I \in M^c : p(I) > \epsilon\}), \end{aligned}$$

where $A = A_\alpha(\Phi) = \{I : \|\Phi_I^T \phi_i\|_2^2 > \alpha \text{ for some } i \in I^c\}$ is the set of supports appearing in the definition of the WSINC property. If $I \in M \cap A$, i.e., it supports both StRIP and SINC properties, then (11) implies that $p(I) \leq \epsilon$, so the first term on the right-hand side equals 0. The third term refers to supports with no SINC property, whose total probability is $\leq \epsilon$. Estimating the second term by the Markov inequality, we have

$$(12) \quad P_{R_k}(\{I \in M \cap A^c : p(I) > \epsilon\}) \leq \frac{\mathbf{E}_{R_k}[p(I), \mathbf{1}(I \in M \cap A^c)]}{\epsilon}$$

where $\mathbf{1}(\cdot)$ denotes the indicator random variable. We have

$$(13) \quad \mathbf{E}_{R_k}[p(I), I \in M \cap A^c] = \mathbf{E}_{R_k}[p(I) \mathbf{1}(I \in M \cap A^c)] = \sum_{I \in M \cap A^c} \frac{1}{\binom{N}{k}} p(I),$$

Let us first estimate $p(I)$ for $I \in M \cap A^c$ by invoking Hoeffding's inequality (9):

$$\begin{aligned} p(I) &= P_{R^k}(\exists i \in I^c, |v_i| > 1/2) \leq \sum_{i \in I^c} P_{R^k}(|v_i| > 1/2) \\ &\leq \sum_{i \in I^c} 2 \exp\left(-\frac{1}{8\|\mathbf{s}_i\|_2^2}\right) \\ &\stackrel{(10)}{\leq} \sum_{i \in I^c} 2 \exp\left(-\frac{(1-\delta)^2}{8\|\Phi_I^T \phi_i\|_2^2}\right) \\ &= 2(N-k) \sum_{t \in \mathcal{B}(\Phi)} \exp\left(-\frac{(1-\delta)^2}{8t^2}\right) P_{R'_k}(\|\Phi_I^T \phi_i\|_2 = t \mid I). \end{aligned}$$

Substituting this result into (13), we obtain

$$\begin{aligned} \mathbf{E}_{R_k}[p(I), \{I \in M \cap A^c\}] &\leq 2(N-k) \sum_{t \in \mathcal{B}(\Phi)} \exp\left(-\frac{(1-\delta)^2}{8t^2}\right) \sum_{I \in M \cap A^c} \frac{1}{\binom{N}{k}} P_{R'_k}(\|\Phi_I^T \phi_i\|_2 = t \mid I) \\ &\leq 2(N-k) \sum_{t \in \mathcal{B}(\Phi)} \exp\left(-\frac{(1-\delta)^2}{8t^2}\right) P_{R'_k}(I \in A^c, \|\Phi_I^T \phi\|_2 = t) \\ &\leq 2\epsilon^2 \end{aligned}$$

where the last step is on account of (12) and the WSINC assumption. ■

Proof of Theorem 2.5: Define the set B by

$$B = \{I \in R_k : P_{R^k}(\|v_{I^c}\|_\infty > 1/2 \mid I) > \epsilon\}.$$

Recall that Theorem 2.5 is stated with respect to the random signal \mathbf{x} . Therefore, let us estimate the probability

$$\begin{aligned} & P_{R_k \times R^k}(\{(I, \mathbf{x}) : \|\mathbf{v}_{I^c}\|_\infty > 1/2\}) \\ &= \sum_{I \in \mathcal{P}_k(N)} P_{R_k \times R^k}(\{\mathbf{x} : \|\mathbf{v}_{I^c}\|_\infty > 1/2\} \mid I) P_{R_k \times R^k}(I) \\ &= \sum_{I \in B^c} P_{R^k}(\{\mathbf{x} : \|\mathbf{v}_{I^c}\|_\infty > 1/2\} \mid I) P_{R_k}(I) + \sum_{I \in B} P_{R^k}(\{\mathbf{x} : \|\mathbf{v}_{I^c}\|_\infty > 1/2\} \mid I) P_{R_k}(I). \end{aligned}$$

We have $P_{R^k}(\{\mathbf{x} : \|\mathbf{v}_{I^c}\|_\infty > 1/2\} \mid I) < \epsilon$ from Lemma 2.4 and $P_{R_k}(B) \leq 3\epsilon$ from Lemma 2.6, so

$$P_{R_k \times R^k}(\{(I, \mathbf{x}) : \|\mathbf{v}_{I^c}\|_\infty > 1/2\}) < \epsilon(1 + 3\epsilon) < 4\epsilon.$$

This implies that with probability $1 - 4\epsilon$ the signal \mathbf{x} chosen from the generic random signal model satisfies the conditions of Lemma 2.3, i.e.,

$$\|\mathbf{x}_{I^c} - \hat{\mathbf{x}}_{I^c}\|_1 \leq 4\|\mathbf{x}_{I^c}\|_1.$$

This completes the proof. ■

3. INCOHERENCE PROPERTIES AND LASSO

In this section we prove that sparse signals can be approximately recovered from low-dimensional observations using Lasso if the sampling matrices have statistical incoherence properties. The result is a modification of the methods developed in [15, 49] in that we prove that the conditions used there to bound the error of the Lasso estimate hold with high probability if Φ has both StRIP and SINC properties. The precise claim is given in the following statement.

Theorem 3.1. *Let \mathbf{x} be a random k -sparse signal whose support satisfies the two properties of the generic random signal model S_k . Denote by $\hat{\mathbf{x}}$ its estimate from $\mathbf{y} = \Phi\mathbf{x} + \mathbf{z}$ via Lasso (3), where \mathbf{z} is a i.i.d. Gaussian vector with zero mean and variance σ^2 and where $\lambda = 2\sqrt{2\log N}$. Suppose that $k \leq \frac{c_0 N}{\|\Phi\|^2 \log N}$, where c_0 is a positive constant, and that the matrix Φ satisfies the following two properties:*

- (1) Φ is $(k, \frac{1}{2}, \epsilon)$ -StRIP.
- (2) Φ is $(k, \frac{1}{128 \log(N/2\epsilon)}, \epsilon)$ -SINC.

Then we have

$$\|\Phi\mathbf{x} - \Phi\hat{\mathbf{x}}\|_2^2 \leq C_0 k \log N \sigma^2,$$

with probability at least $1 - 3\epsilon - \frac{1}{N\sqrt{2\pi\log N}} - N^{-a}$, where $C_0 > 0$ is an absolute constant and $a = 0.15 \log(2N/\epsilon) - 1$.

The following theorem is implicit in [15], see Theorem 1.2 and Sect 3.2 in that paper.

Theorem 3.2. (Candès and Plan) *Suppose that \mathbf{x} is a k -sparse signal drawn from the model S_k , where*

$$k \leq \frac{c_0 N}{\|\Phi\|^2 \log N},$$

where $c_0 > 0$ is a constant. Let $I \subset [N]$ be the support of \mathbf{x} and suppose the following three conditions are satisfied:

- (1) $\|(\Phi_I^T \Phi_I)^{-1}\| \leq 2$.
- (2) $\|\Phi^T \mathbf{z}\|_{\ell_\infty} \leq 2\sqrt{\log N}$.
- (3) $\|\Phi_{I^c}^T \Phi_I (\Phi_I^T \Phi_I)^{-1} \Phi_{I^c}^T \mathbf{z}\|_{\ell_\infty} + \sqrt{8 \log N} \|\Phi_{I^c}^T \Phi_I (\Phi_I^T \Phi_I)^{-1} \text{sgn}(\mathbf{x}_I)\|_{\ell_\infty} \leq (2 - \sqrt{2})\sqrt{2 \log N}$.

Then

$$\|\Phi\mathbf{x} - \Phi\hat{\mathbf{x}}\|_2^2 \leq C_0 k (\log N) \sigma^2,$$

where C_0 is an absolute constant.

Our aim will be to prove that conditions (1)-(3) of this theorem hold with large probability under the assumptions of Theorem 3.1.

First, it is clear that $\|\Phi^T \mathbf{z}\|_\infty \leq 2\sqrt{\log N}$ with probability at least $1 - (N\sqrt{2\pi\log N})^{-1}$. This follows simply because \mathbf{z} is an independent Gaussian vector, and has been discussed in [15] (this is also the reason for selecting the particular value of λ_N). The main part of the argument is contained in the following lemma whose proof uses some ideas of [15].

Lemma 3.3. Suppose that $1/2 \leq \|\Phi_I^T \Phi_I - \text{Id}\| \leq 3/2$ and that for all $i \in I^c$,

$$\|\Phi_I^T \phi_i\|_2^2 \leq (128 \log(2N/\epsilon))^{-1}.$$

Then Condition (3) of Theorem 3.2 holds with probability at least $1 - \epsilon - N^{-a}$ for $a = 0.15 \log(2N/\epsilon) - 1$.

Proof. Let $i \in I^c$. Define $Z_{0,i} = \langle \mathbf{w}_i, \text{sgn}(\mathbf{x}_I) \rangle$ and $Z_{1,i} = \langle \mathbf{w}'_i, \mathbf{z} \rangle$, where

$$\begin{aligned} \mathbf{w}_i &= (\Phi_I^T \Phi_I)^{-1} \Phi_I^T \phi_i, \\ \mathbf{w}'_i &= \Phi_I (\Phi_I^T \Phi_I)^{-1} \Phi_I^T \phi_i. \end{aligned}$$

Let $Z_0 = \max_{i \in I^c} |Z_{0,i}|$ and $Z_1 = \max_{i \in I^c} |Z_{1,i}|$. We will show that with high probability $Z_0 \leq 1/4$ and $Z_1 \leq (1.5 - \sqrt{2})\sqrt{2 \log N}$ which will imply the lemma. We compute

$$\begin{aligned} \|\mathbf{w}_i\|_2 &\leq \|(\Phi_I^T \Phi_I)^{-1}\| \|\Phi_I^T \phi_i\|_2 \leq 2 \frac{1}{8\sqrt{2 \log(2N/\epsilon)}} \\ &= \frac{1}{4\sqrt{2 \log(2N/\epsilon)}}, \end{aligned}$$

and

$$\begin{aligned} \|\mathbf{w}'_i\|_2 &\leq \|\Phi_I\| \|(\Phi_I^T \Phi_I)^{-1}\| \|\Phi_I^T \phi_i\|_2 \leq \sqrt{\frac{3}{2}} \frac{2}{8\sqrt{2 \log(2N/\epsilon)}} \\ &= \frac{\sqrt{3}}{8\sqrt{\log(2N/\epsilon)}} \end{aligned}$$

for all $i \in I^c$. Let $a_1 = 1.5 - \sqrt{2}$. Since $Z_{1,i} \sim \mathcal{N}(0, \|\mathbf{w}'_i\|_2^2)$, we have

$$\begin{aligned} \Pr(Z_1 > a_1 \sqrt{2 \log N}) &\leq (N - k) \Pr(|Z_{1,i}| > a_1 \sqrt{2 \log N}) \\ &\leq \frac{2(N - k) \|\mathbf{w}'_i\|_2}{a_1 \sqrt{2\pi(2 \log N)}} e^{-\frac{64}{3} a_1^2 \log N \log(2N/\epsilon)} \\ &\leq \frac{2.1}{\sqrt{(2 \log N) \log(2N/\epsilon)}} N^{-0.15 \log(2N/\epsilon) + 1} \\ &\leq N^{-a}. \end{aligned}$$

(the multiplier in front of the exponent is less than 1 for all $N > 4$ and $\epsilon < 1$). Further, since the signs $\text{sgn}(x_i)$, $i \in I$ are uniform i.i.d. random variables, we have

$$\begin{aligned} \Pr(Z_0 > 1/4) &\leq (N - k) \Pr(|\langle \mathbf{w}_i, \text{sgn}(\mathbf{x}_I) \rangle| > 1/4) \\ &\leq 2(N - k) e^{-1/(32\|\mathbf{w}_i\|_2^2)} \\ &< \epsilon. \end{aligned}$$

The proof is complete. ■

Theorem 3.1 is now easily established. Indeed, the assumptions of Lemma 3.3 are satisfied with probability at least $1 - 2\epsilon$. The claim of the theorem follows from the above arguments.

4. SUFFICIENT CONDITIONS FOR STATISTICAL INCOHERENCE PROPERTIES

As discussed earlier, recovery properties of sampling matrices in linear programming decoding procedures are controlled by the coherence parameter $\mu(\Phi) = \max_{i,j} \mu_{ij}$. In particular, the Gershgorin theorem implies that the condition $\mu = O(k^{-1})$ is sufficient for stable and robust recovery of signals with sparsity k . In this section we show that this result can be improved to $\mu = O(k^{-1/4})$ in that the matrix satisfies the StRIP and SINC conditions. The results of Sect. 2 then imply stable recovery of generic random k -sparse signals using linear programming decoding.

Let Φ be an $m \times N$ sampling matrix with columns ϕ_i , $i = 1, \dots, N$. As above, let $\mu_{ij} = |\phi_i^T \phi_j|$. Call the matrix Φ *coherence-invariant* the set $M_i := \{\mu_{ij}, j \in [N] \setminus i\}$ is independent of i . Observe that most known constructions of sampling matrices satisfy this property. This includes matrices constructed from linear codes [25, 6, 42], chirp matrices and various Reed-Muller matrices [3, 12], as well as subsampled Fourier matrices [31]. Our arguments change slightly

if the matrix is not coherence-invariant. To deal simultaneously with both cases, define the parameter $\theta = \theta(\Phi)$ as $\theta = \bar{\mu}^2$ if Φ is coherence-invariant and $\theta = \bar{\mu}_{\max}^2$ otherwise.

The next theorem gives sufficient conditions for the SINC property in terms of coherence parameters of Φ .

Theorem 4.1. *Let Φ be an $m \times N$ matrix with unit-norm columns, coherence μ and square coherence θ . Suppose that Φ is coherence-invariant,*

$$(14) \quad \mu^4 \leq \frac{(1-a)^2 \beta^2}{32k(\log 2N/\epsilon)^3} \quad \text{and} \quad \theta \leq \frac{a\beta}{k \log(2N/\epsilon)},$$

where $\beta > 0$ and $0 < a < 1$ are any constants. Then Φ has the (k, α, ϵ) -SINC property with $\alpha = \beta / \log(2N/\epsilon)$.

Before proving this theorem we will introduce some notation. Fix $j \in [N]$ and let $I_j = \{i_1, i_2, \dots, i_k\}$ be a random k -subset such that $j \notin I_j$. The subsets I_j are chosen from the set $[N-1]$ with uniform distribution. Define random variables $Y_{j,l} = \mu_{j,i_l}^2, l = 1, \dots, k$. Next define a sequence of random variables $Z_{j,t}, t = 0, 1, \dots, k$, where

$$Z_{j,0} = \mathbb{E}_{I_j} \sum_{l=1}^k Y_{j,l}, \quad Z_{j,t} = \mathbb{E}_{I_j} \left(\sum_{l=1}^k Y_{j,l} \mid Y_{j,1}, Y_{j,2}, \dots, Y_{j,t} \right), \quad t = 1, 2, \dots, k.$$

From the assumption of coherence invariance, the variables $Z_{j,t}$ for different j are stochastically equivalent. Let

$$Z_t = \mathbb{E}_j Z_{j,t} = \mathbb{E}_{R'_k} \left(\sum_{l=1}^k Y_{j,l} \mid Y_{j,1}, Y_{j,2}, \dots, Y_{j,t} \right), \quad t = 1, \dots, k.$$

The random variables Z_t are defined on the set of $(k+1)$ -subsets of $[N]$ with probability distribution $P_{R'_k}$. We will show that they form a Doob martingale. Begin with defining a sequence of σ -algebras $\mathcal{F}_t, t = 0, 1, \dots, k$, where $\mathcal{F}_0 = \{\emptyset, [N]\}$ and $\mathcal{F}_t, t \geq 1$ is the smallest σ -algebra with respect to which the variables $Y_{j,1}, \dots, Y_{j,t}$ are measurable (thus, \mathcal{F}_t is formed of all subsets of $[N]$ of size $\leq t+1$). Clearly, $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \dots \subset \mathcal{F}_k$, and for each t , Z_t is a bounded random variable that is measurable with respect to \mathcal{F}_t . Observe that

$$(15) \quad Z_0 = \mathbb{E}_j Z_{j,0} = \mathbb{E}_{R'_k} \sum_{l=1}^k \mu_{j,i_l}^2 = \sum_{l=1}^k \mathbb{E}_{R'_k} \mu_{j,i_l}^2 = k \bar{\mu}^2$$

$$(16) \quad \leq k \bar{\mu}_{\max}^2,$$

where (15) assumes coherence invariance, and (16) is valid independently of that assumption.

Lemma 4.2. *The sequence $(Z_t, \mathcal{F}_t)_{t=0,1,\dots,k}$ forms a bounded-differences martingale, namely $\mathbb{E}_{R'_k}(Z_t \mid Z_0, Z_1, \dots, Z_{t-1}) = Z_{t-1}$ and*

$$|Z_t - Z_{t-1}| \leq 2\mu^2 \left(1 + \frac{k}{N-k-2} \right), \quad t = 1, \dots, k.$$

Proof. In the proof we write \mathbb{E} instead of $\mathbb{E}_{R'_k}$. We have

$$\begin{aligned} Z_t &= \mathbb{E} \left(\sum_{l=1}^k Y_{j,l} \mid \mathcal{F}_t \right) = \sum_{l=1}^t Y_{j,l} + \mathbb{E} \left(\sum_{l=t+1}^k Y_{j,l} \mid \mathcal{F}_t \right) \\ &= Z_{t-1} + Y_{j,t} + \mathbb{E} \left(\sum_{l=t+1}^k Y_{j,l} \mid \mathcal{F}_t \right) - \mathbb{E} \left(\sum_{l=t}^k Y_{j,l} \mid \mathcal{F}_{t-1} \right). \end{aligned}$$

Next,

$$\begin{aligned}
\mathbb{E}(Z_t \mid Z_0, Z_1, \dots, Z_{t-1}) &= Z_{t-1} + \mathbb{E}(Y_{j,t} \mid Z_0, Z_1, \dots, Z_{t-1}) + \mathbb{E}\left(\mathbb{E}\left(\sum_{l=t+1}^k Y_{j,l} \mid \mathcal{F}_t\right) \mid Z_0, \dots, Z_{t-1}\right) \\
&\quad - \mathbb{E}\left(\mathbb{E}\left(\sum_{l=t}^k Y_{j,l} \mid \mathcal{F}_{t-1}\right) \mid Z_0, \dots, Z_{t-1}\right) \\
&= Z_{t-1} + \mathbb{E}(Y_{j,t} \mid Z_0, \dots, Z_{t-1}) \\
&\quad + \mathbb{E}\left(\sum_{l=t+1}^k Y_{j,l} \mid Z_0, \dots, Z_{t-1}\right) - \mathbb{E}\left(\sum_{l=t}^k Y_{j,l} \mid Z_0, \dots, Z_{t-1}\right) \\
&= Z_{t-1},
\end{aligned}$$

which is what we claimed.

Next we prove a bound on the random variable $|Z_t - Z_{t-1}|$. We have

$$\begin{aligned}
|Z_t - Z_{t-1}| &= \left| \mathbb{E}\left(\sum_{l=1}^k Y_{j,l} \mid \mathcal{F}_t\right) - \mathbb{E}\left(\sum_{l=1}^k Y_{j,l} \mid \mathcal{F}_{t-1}\right) \right| \\
&\leq \max_{a,b} \left| \mathbb{E}\left(\sum_{l=1}^k Y_{j,l} \mid \mathcal{F}_{t-1}, Y_{t,l} = a\right) - \mathbb{E}\left(\sum_{l=1}^k Y_{j,l} \mid \mathcal{F}_{t-1}, Y_{t,l} = b\right) \right| \\
&= \max_{a,b} \left| \sum_{l=1}^k \left(\mathbb{E}(Y_{j,l} \mid \mathcal{F}_{t-1}, Y_{t,l} = a) - \mathbb{E}(Y_{j,l} \mid \mathcal{F}_{t-1}, Y_{t,l} = b) \right) \right| \\
&= \max_{a,b} \left| a - b + \sum_{l=t+1}^k \left(\mathbb{E}(Y_{j,l} \mid \mathcal{F}_{t-1}, Y_{t,l} = a) - \mathbb{E}(Y_{j,l} \mid \mathcal{F}_{t-1}, Y_{t,l} = b) \right) \right| \\
&\leq \left| 2\mu^2 + \sum_{l=t+1}^k \frac{2\mu^2}{N-l-2} \right| \\
&= 2\mu^2 \frac{N-2}{N-k-2}
\end{aligned}$$

■

To prove Theorem 4.1 we use the Azuma-Hoeffding inequality (see, e.g., [41]).

Proposition 4.3. (Azuma-Hoeffding) *Let X_0, \dots, X_{k-1} be a martingale with $|X_i - X_{i-1}| \leq a_i$ for each i , for suitable constants a_i . Then for any $\nu > 0$,*

$$\Pr\left(\left|\sum_{t=1}^{k-1} (X_t - X_{t-1})\right| \geq \nu\right) \leq 2 \exp \frac{-\nu^2}{2 \sum a_i^2}.$$

Proof of Theorem 4.1: Bounding large deviations for the sum $|\sum_{t=1}^k (Z_t - Z_{t-1})| = |Z_k - Z_0|$, we obtain

$$(17) \quad \Pr(|Z_k - Z_0| > \nu) \leq 2 \exp \left(- \frac{\nu^2}{8\mu^4 k \left(\frac{N-2}{N-k-2}\right)^2} \right),$$

where the probability is computed with respect to the choice of *ordered* $(k+1)$ -tuples in $[N]$ and $\nu > 0$ is any constant. Assume coherence invariance. Using (15) and the inequality $(N-2)/(N-k-2) < 2$ valid for all $k < \frac{N}{2} - 1$, we obtain

$$\Pr(Z_k \geq \nu + k\bar{\mu}^2) \leq \Pr(|Z_k - k\bar{\mu}^2| \geq \nu) \leq 2 \exp \left(- \frac{\nu^2}{32\mu^2 k} \right).$$

Now take $\beta > 0$ and $\nu = \frac{\beta}{\log(2N/\epsilon)} - k\bar{\mu}^2$. Suppose that for some $a \in (0, 1)$

$$(18) \quad k\mu^4 \leq \frac{((1-a)\beta)^2}{32} \left(\log \frac{2N}{\epsilon} \right)^{-3}, \quad k\bar{\mu}^2 \leq \frac{a\beta}{\log(2N/\epsilon)},$$

then we obtain

$$(19) \quad \Pr \left(\|\Phi_{I_j}^T \phi_j\|_2^2 \geq \frac{\beta}{\log(2N/\epsilon)} \right) \leq 2 \exp \left(-\frac{\nu^4}{32\mu^4 k} \right) \leq \frac{\epsilon}{N}$$

Now the first claim of Theorem 4.1 follows by the union bound with respect to the choice of the index j .

Assume that Φ does not satisfy the invariance condition. Then we rely on (16) and repeat the above argument with respect to $\bar{\mu}_{\max}^2$. ■

The above proof contains the following statement.

Corollary 4.4. *Let Φ be an $m \times N$ matrix with coherence μ and $\theta = \bar{\mu}^2$ or $\bar{\mu}_{\max}^2$, as appropriate. Let $a \in (0, 1)$ and $\beta > 0$ be any constants. Suppose that for $\alpha < \beta \log_2 e$,*

$$\mu^4 \leq \frac{(1-a)^2 \alpha^3}{32\beta k}, \quad k\theta \leq a\alpha.$$

Then $P_{R_k}(\sum_{l=1}^k \mu_{i_l, j}^2 \geq \alpha) \leq 2e^{-\beta/\alpha}$.

Proof. Denote $\alpha = \beta/(\log(2N/\epsilon))$, then $\epsilon/N = 2e^{-\beta/\alpha}$. The claim is obtained by substituting α in (18)-(19). ■

We note that this corollary follows directly from the SINC property under our assumptions on coherence and mean square coherence. We observe that the SINC property naturally implies some StRIP condition as given in the following theorem.

Theorem 4.5. *Let Φ be an $m \times N$ matrix. Let $I \subset [N]$ be a random ordered k -subset and suppose that for all $j \in I$, $\Pr(\sum_{m=1}^{k-1} \mu_{j, i_m}^2 > \delta^2/k) < \epsilon_1/k$. Then Φ is a (k, δ, ϵ_1) -StRIP matrix.*

Proof. Given I let $H(I) = \Phi_I^T \Phi_I - \text{Id}$ be the “hollow Gram matrix”. Let $B = \{I : \|H(I)\|_2 > \delta\} \subset \mathcal{P}_k(N)$. We need to prove that $P_{R_k}(B) \leq \epsilon$. Let (e_1, \dots, e_k) be the standard basis of \mathbb{R}^k . Define a subset $C \subset \mathcal{P}_k(N)$ as follows:

$$C = \{I : \exists i \in I \text{ s.t. } \|H(I)e_i\|_2 \geq \delta/\sqrt{k}\}$$

Let us show that $B \subseteq C$ by proving $C^c \subseteq B^c$. Indeed, if $I \in C^c$, then we have

$$\begin{aligned} \|H(I)\| &= \max_{\|x\|_2=1} \|H(I)x\|_2 = \max_{\|x\|_2=1} \|H(I)(x_1 e_1 + x_2 e_2 + \dots + x_k e_k)\| \\ &\leq \max_{\|x\|_2=1} \sum_l |x_l| \|H(I)e_l\|_2 \\ &\leq \max_{\|x\|_2=1} \|x\|_1 \max_{1 \leq l \leq k} \|H(I)e_l\|_2 \\ &\leq \sqrt{k} \max_{1 \leq l \leq k} \|H(I)e_l\|_2 \\ &\leq \delta, \end{aligned}$$

which implies $I \in B^c$. Now since $B \subseteq C$, we only need to show that $P_{R_k}(C) \leq \epsilon$.

Careful readers may have already noticed that the target quantity $P_{R_k}(C)$ uses a different probability measure from that in theorem’s assumption. We note that a change of measure is actually inevitable since the probability measure in Azuma-Hoeffding’s inequality we used in Proposition 4.3 is with respect to ordered k -tuples while that in the definition of StRIP is with respect to unordered ones. In the following, we provide a rigorous calculation that supports this measure transformation.

For any $I \in C$, by definition, there exists at least one $l \in I$ such that $\|H_I e_l\| \geq \delta/\sqrt{k}$. Among such l , let $i(I)$ be the smallest one $i(I) = \min\{l \in I : \|H_I e_l\|_2 \geq \delta/\sqrt{k}\}$. Now we define a map from an unordered k -tuple $I \in C \subseteq \mathcal{P}_k(N)$ to a set of ordered k -tuples $Q(I) = \{(i_1, \dots, i_k) : (i_1, \dots, i_{k-1}) = \sigma(I \setminus i(I)), \sigma \in S_{k-1}\}$, where S_{k-1} denotes the set of all permutations of $k-1$ elements. Obviously, $|Q(I)| = (k-1)!$ for all I , and $Q(I_1) \cap Q(I_2) = \emptyset$ for distinct k -subsets I_1, I_2 . Moreover, if $(i_1, \dots, i_k) \in Q(I)$, then $\|H(I)e_k\|_2 \geq \delta/\sqrt{k}$ or $\sum_{l=1}^{k-1} \mu_{i_l, i_k}^2 > \delta^2/k$. Therefore

$$\bigcup_{I \in C} Q(I) \subseteq \{(i_1, \dots, i_k) \subset [N] : \sum_{l=1}^{k-1} \mu_{i_l, i_k}^2 > \delta^2/k\}$$

Now compute

$$\begin{aligned}
P_{R_k}(B) &= \frac{|B|}{\binom{N}{k}} \leq \frac{|C|(k-1)!}{\binom{N}{k}(k-1)!} = \frac{\sum_{I \in C} |Q(I)|}{\binom{N}{k}(k-1)!} \\
&= \frac{|\bigcup_{I \in C} Q(I)|}{\binom{N}{k}(k-1)!} \\
&\leq \frac{k}{k! \binom{N}{k}} \left| \left\{ (i_1, \dots, i_k) \subset [N] : \sum_{l=1}^{k-1} \mu_{i_l, i_k}^2 > \delta^2/k \right\} \right| \\
&= k \Pr\left(\sum_{m=1}^{k-1} \mu_{j, i_m}^2 > \delta^2/k\right).
\end{aligned}$$

By the assumption of the theorem the last expression is at most ϵ which proves our claim. ■

Theorem 4.5 implies the following

Corollary 4.6. *Let Φ be an $m \times N$ matrix. If*

$$\theta \leq \frac{a\delta^2}{k^2}, \quad \text{and} \quad \mu^4 \leq \frac{(1-a)^2\delta^4}{32k^3 \log(2k/\epsilon_1)},$$

where $0 < a < 1$, then Φ is (k, δ, ϵ_1) -StRIP.

Proof. Take $\epsilon_1 = 2ke^{-\beta/\alpha}$, then $\beta = \frac{\delta^2}{k} \log(2k/\epsilon_1)$. The claim is obtained by substituting this value into the conditions of Corollary 4.4. ■

Observe that the sufficient condition for the (k, δ) -RIP property from the Gershgorin theorem is $\mu < \delta/k$, so the result of Corollary 4.6 gives a better result, namely $\mu = O(k^{-3/4})$. At the same time, Tropp's result in [49, Thm. B] implies that the matrix Φ is (k, δ, ϵ) -StRIP under a weaker (i.e., more inclusive) condition. Below we improve upon these results by analyzing the StRIP property directly rather than relying on the SINC condition.

Theorem 4.7. *Let Φ be an $m \times N$ matrix and let $\theta = \bar{\mu}^2$ or $\theta = \bar{\mu}_{\max}^2$, depending on whether Φ is coherence-invariant or not. Let $\epsilon < \min\{1/k, e^{1-1/\log^2}\}$ and suppose that Φ satisfies*

$$(20) \quad k\mu^4 \leq \frac{1}{\log^2(1/\epsilon)} \min\left(\frac{(1-a)^2b^2}{32 \log(2k) \log(e/\epsilon)}, c^2\right) \quad \text{and} \quad k\theta \leq \frac{ab}{\log(1/\epsilon)},$$

where $a, b, c \in (0, 1)$ are constants such that

$$(21) \quad \sqrt{a} + \sqrt{2ab} + \sqrt{c} + \frac{2k}{N} \|\Phi\|^2 \leq e^{-1/4} \delta / 6\sqrt{2}.$$

Then Φ is (k, δ, ϵ) -StRIP.

The proof relies on several results from [49]. The following theorem is a modification of Theorem 25 in that paper. Below R denotes a linear operator that performs a restriction to k coordinates chosen according to some rule (e.g., randomly). Its domain is determined by the context. Its adjoint R^* acts on \mathbb{R}^k by padding the k -vector with the appropriate number of zeros.

Theorem 4.8. (Decoupling of the spectral norm) *Let A be a $2N \times 2N$ symmetric matrix with zero diagonal. Let $\eta \in \{0, 1\}^{2N}$ be a random vector with N components equal to one. Define the index sets $T_1(\eta) = \{i : \eta_i = 0\}$, $T_2(\eta) = \{i : \eta_i = 1\}$. Let R be a random restriction to k coordinates. For any $q \geq 1$ we have*

$$(22) \quad (\mathbb{E} \|RAR^*\|^q)^{1/q} \leq 2 \max_{k_1+k_2=k} \mathbb{E}_\eta (\mathbb{E} \|R_1 A_{T_1(\eta) \times T_2(\eta)} R_2^*\|^q)^{1/q},$$

where $A_{T_1(\eta) \times T_2(\eta)}$ denotes the submatrix of A indexed by $T_1(\eta) \times T_2(\eta)$ and the matrices R_i are independent restrictions to k_i coordinates from T_i , $i = 1, 2$.

When A has order $(2N+1) \times (2N+1)$, then an analogous result holds for partitions into blocks of size N and $N+1$.

Inequality (22) is implicitly proved in the proof of the decoupling theorem (Theorem 9) [49]. The ideas behind it are due to [38].

The next lemma is due to Tropp [48] and Rudelson and Vershinin [44].

Lemma 4.9. *Suppose that A is a matrix with N columns and let R be a random restriction to k coordinates. Let $q \geq 2, p = \max(2, 2 \log(\text{rk } AR^*), q/2)$. Then*

$$(\mathbb{E} \|AR^*\|^q)^{1/q} \leq 3\sqrt{p}(E \|AR^*\|_{1 \rightarrow 2}^q)^{1/q} + \sqrt{\frac{k}{N}} \|A\|$$

where $\|\cdot\|_{1 \rightarrow 2}$ is the maximum column norm.

The following lemma is a simple application of Markov's inequality, a similar result can be found in [38], Lemma 4.10; see also [49].

Lemma 4.10. *Let $q, \lambda > 0$ and let ξ_q be a positive function of q . Suppose that Z is a positive random variable whose q th moment satisfies the bound*

$$(\mathbb{E} Z^q)^{1/q} \leq \xi_q \sqrt{q} + \lambda.$$

Then

$$P(Z \geq e^{1/4}(\xi_q \sqrt{q} + \lambda)) \leq e^{-q/4}.$$

Proof: By the Markov inequality,

$$P\left(Z \geq e^{1/4}(\xi_q \sqrt{q} + \lambda)\right) \leq \frac{\mathbb{E} Z^q}{(e^{1/4}(\xi_q \sqrt{q} + \lambda))^q} \leq \left(\frac{\xi_q \sqrt{q} + \lambda}{e^{1/4}(\xi_q \sqrt{q} + \lambda)}\right)^q = e^{-q/4}. \quad \blacksquare$$

The main part of the proof is contained in the following lemma.

Lemma 4.11. *Let Φ be an $m \times N$ matrix with coherence parameter μ . Suppose that for some $0 < \epsilon_1, \epsilon_2 < 1$*

$$(23) \quad P_{R_k^*}(\{(I, i) : \|\Phi_I^T \phi_i\|^2 \geq \epsilon_1\} \mid i) \leq \epsilon_2.$$

Let R be a random restriction to k coordinates and $H = \Phi^T \Phi - \text{Id}$. For any $q \geq 2, p = \max(2, 2 \log(\text{rk } RHR^), q/2)$ we have*

$$(24) \quad (\mathbb{E} \|RHR^*\|^q)^{1/q} \leq 6\sqrt{p}(\sqrt{\epsilon_1} + (k\epsilon_2)^{1/q} \mu \sqrt{k} + \sqrt{2k\theta}) + \frac{2k}{N} \|\Phi\|^2.$$

Proof. We begin with setting the stage to apply Theorem 4.8. Let $\eta \in \{0, 1\}^N$ be a random vector with $N/2$ ones and let R_1, R_2 be random restrictions to k_i coordinates in the sets $T_i(\eta), i = 1, 2$, respectively. Denote by $\text{supp}(R_i), i = 1, 2$ the set of indices selected by R_i and let $H(\eta) := H_{T_1(\eta) \times T_2(\eta)}$. Let $q \geq 1$ and let us bound the term $\mathbb{E}_\eta(\mathbb{E} \|R_1 H(\eta) R_2\|^q)^{1/q}$ that appears on the right side of (22). The expectation in the q -norm is computed for two random restrictions R_1 and R_2 that are conditionally independent given η . Let \mathbb{E}_i be the expectation with respect to $R_i, i = 1, 2$. Given η we can evaluate these expectations in succession and apply Lemma 4.9 to \mathbb{E}_2 :

$$\begin{aligned} \mathbb{E}_\eta(\mathbb{E} \|R_1 H(\eta) R_2^*\|^q)^{1/q} &= \mathbb{E}_\eta \left[\mathbb{E}_1(\mathbb{E}_2 \|R_1 H(\eta) R_2^*\|^q)^{q/q} \right]^{1/q} \\ &\leq \mathbb{E}_\eta \left\{ \mathbb{E}_1 \left[3\sqrt{p}(\mathbb{E}_2 \|R_1 H(\eta) R_2^*\|_{1 \rightarrow 2}^q)^{1/q} + \sqrt{\frac{2k_2}{N}} \|R_1 H(\eta)\| \right]^q \right\}^{1/q} \\ &\leq \mathbb{E}_\eta \left\{ 3\sqrt{p} \left[\mathbb{E}_1(\mathbb{E}_2 \|R_1 H(\eta) R_2^*\|_{1 \rightarrow 2}^q)^{1/q} + \sqrt{\frac{2k_2}{N}} [\mathbb{E}_1 \|R_1 H(\eta)\|^q]^{1/q} \right] \right\} \end{aligned}$$

where on the last line we used the Minkowski inequality (recall that the random variables involved are finite). Now use Lemma 4.9 again to obtain

$$(25) \quad \begin{aligned} \mathbb{E}_\eta(\mathbb{E} \|R_1 H(\eta) R_2^*\|^q)^{1/q} &\leq 3\sqrt{p} \mathbb{E}_\eta \left[\mathbb{E}_1 \mathbb{E}_2 \|R_1 H(\eta) R_2^*\|_{1 \rightarrow 2}^q \right]^{1/q} + 3\sqrt{\frac{2k_2 p}{N}} \mathbb{E}_\eta(\mathbb{E}_1 \|H(\eta)^* R_1^*\|_{1 \rightarrow 2}^q)^{1/q} \\ &\quad + \sqrt{\frac{4k_1 k_2}{N^2}} \mathbb{E}_\eta \|H(\eta)^*\|. \end{aligned}$$

Let us examine the three terms on the right-hand side of the last expression. Let $\eta(R_2)$ be the random vector conditional on the choice of k_2 coordinates. The sample space for $\eta(R_2)$ is formed of all the vectors $\eta \in \{0, 1\}^N$ such that $\text{supp}(R_2) \subset T_2(\eta)$. In other words, this is a subset of the sample space $\{0, 1\}^N$ that is compatible with a given R_2 .

The random restriction R_1 is still chosen out of $T_1(\eta)$ independently of R_2 . Denote by \tilde{R} a random restriction to k_1 indices in the set $(\text{supp}(R_2))^c$ and let $\tilde{\mathbf{E}}$ be the expectation computed with respect to it. We can write

$$\begin{aligned} \mathbf{E}_\eta(\mathbf{E}_1 \mathbf{E}_2 \|R_1 H(\eta) R_2^*\|_{1 \rightarrow 2}^q)^{1/q} &\leq (\mathbf{E}_\eta \mathbf{E}_1 \mathbf{E}_2 \|R_1 H(\eta) R_2^*\|_{1 \rightarrow 2}^q)^{1/q} \\ &= (\mathbf{E}_2 \tilde{\mathbf{E}} \|\tilde{R} H(\eta) R_2^*\|_{1 \rightarrow 2}^q)^{1/q} \end{aligned}$$

Recall that $H_{ij} = \mu_{ij} \mathbf{1}_{\{i \neq j\}}$ and that \tilde{R} and R_2 are 0-1 matrices. Using this in the last equation, we obtain

$$(26) \quad \mathbf{E}_2 \tilde{\mathbf{E}} \|\tilde{R} H(\eta) R_2^*\|_{1 \rightarrow 2}^q \leq \mathbf{E}_2 \tilde{\mathbf{E}} \max_{j \in \text{supp}(R_2)} \left(\sum_{i \in \text{supp}(\tilde{R})} \mu_{ij}^2 \right)^{q/2}.$$

Now let us invoke assumption (23). Recalling that $k_1 < k$, we have

$$P_{R_2, \tilde{R}} \left(\max_{j \in \text{supp}(R_2)} \sum_{i \in \text{supp}(\tilde{R})} \mu_{ij}^2 \geq \epsilon_1 \right) \leq k_2 \epsilon_2.$$

Thus with probability $1 - k_2 \epsilon_2$ the sum in (26) is bounded above by ϵ_1 . For the other instances we use the trivial bound $k_1 \mu^2$. We obtain

$$\begin{aligned} 3\sqrt{p} \mathbf{E}_\eta \mathbf{E}_1 (\mathbf{E}_2 \|R_1 H(\eta) R_2^*\|_{1 \rightarrow 2}^q)^{1/q} &\leq 3\sqrt{p} ((1 - k_2 \epsilon_2) \epsilon_1^{q/2} + k_2 \epsilon_2 (k_1 \mu^2)^{q/2})^{1/q} \\ &\leq 3\sqrt{p} (\epsilon_1^{q/2} + k_2 \epsilon_2 (k_1 \mu^2)^{q/2})^{1/q} \\ &\leq 3\sqrt{p} (\sqrt{\epsilon_1} + (k \epsilon_2)^{1/q} \sqrt{k_1 \mu^2}), \end{aligned}$$

where in the last step we used the inequality $a^q + b^q \leq (a + b)^q$ valid for all $q \geq 1$ and positive a, b . Let us turn to the second term on the right-hand side of (25). Assuming coherence invariance, we observe that

$$\|H(\eta)^* R_1^*\|_{1 \rightarrow 2} = \max_{j \in T_1(\eta)} \|H_{j, T_2(\eta)}\|_2 \leq \max_{j \in [N]} \|H_{j, \cdot}\|_2 = \sqrt{N \bar{\mu}^2}$$

where $H_{j, \cdot}$ denotes the j th row of H and $H_{j, T_2(\eta)}$ is a restriction of the j th row to the indices in $T_2(\eta)$. At the same time, if the dictionary is not coherence-invariant, then in the last step we estimate the maximum norm from above by $\sqrt{N \bar{\mu}_{\max}^2}$, so overall the second term is not greater than $\sqrt{N \theta}$,

Finally, the third term in (25) can be bounded as follows:

$$\begin{aligned} \sqrt{\frac{4k_1 k_2}{N^2}} \mathbf{E}_\eta \|H(\eta)\| &\leq \sqrt{\frac{(k_1 + k_2)^2}{N^2}} \|H\| = \frac{k}{N} \|\Phi^T \Phi - I_N\| \\ &\leq \frac{k}{N} \max(1, \|\Phi\|^2 - 1) \leq \frac{k}{N} \|\Phi\|^2, \end{aligned}$$

where the last step uses the fact that the columns of Φ have unit norm, and so $\Phi^2 \geq N/m > 1$.

Combining all the information accumulated up to this point in (25), we obtain

$$\mathbf{E}_\eta (\mathbf{E} \|R_1 H(\eta) R_2^*\|^q)^{1/q} \leq 3\sqrt{p} (\sqrt{\epsilon_1} + (k \epsilon_2)^{1/q} \mu \sqrt{k} + \sqrt{2k_2 \theta}) + \frac{k}{N} \|\Phi\|^2.$$

Finally, use this estimate in (22) to obtain the claim of the lemma. ■

Proof of Theorem 4.7:

Proof. The strategy is to fix a triple $a, b, c \in (0, 1)$ that satisfies (21) and to prove that (20) implies (k, δ, ϵ) -StRIP. Let $\epsilon_1 = \frac{b}{\log 1/\epsilon}$ and $\epsilon_2 = k^{-1+\log \epsilon}$. In Corollary 4.4 set $\alpha = \epsilon_1$ and $\beta = \alpha \log(2/\epsilon_2)$. Under the assumptions in (20) this corollary implies that

$$P_{R'} \left(\sum_{m=1}^k \mu_{i_m, j}^2 > \epsilon_1 \right) < \epsilon_2.$$

Invoking Lemma 4.11, we conclude that (24) holds with the current values of ϵ_1, ϵ_2 . For any $q \geq 4 \log k$ we have $p = q/2$, and thus (24) becomes

$$(27) \quad (\mathbf{E} \|R H R^*\|^q)^{1/q} \leq 3\sqrt{2q} (\sqrt{\epsilon_1} + (k \epsilon_2)^{1/q} \mu \sqrt{k} + \sqrt{2k_2 \theta}) + 2 \frac{k}{N} \|\Phi\|^2.$$

Introduce the following quantities:

$$\xi_q = 3\sqrt{2} (\sqrt{\epsilon_1} + (k \epsilon_2)^{1/q} \mu \sqrt{k} + \sqrt{2k_2 \theta}) \quad \text{and} \quad \lambda = \frac{2k}{N} \|\Phi\|^2.$$

Now (27) matches the assumption of Lemma 4.10, and we obtain

$$(28) \quad P_{R_k}(\|RHR^*\| \geq e^{1/4}(\xi_q \sqrt{q} + \lambda)) \leq e^{-q/4}.$$

Choose $q = 4 \log(1/\epsilon)$, which is consistent with our earlier assumptions on k , q , and ϵ . With this, we obtain

$$P_{R_k}(\|RHR^*\| \geq e^{1/4}(\xi_q \sqrt{q} + \lambda)) \leq \epsilon.$$

Now observe that $\|RHR^*\| \leq \delta$ is precisely the RIP property for the support identified by the matrix R . Let us verify that the inequality

$$6\sqrt{2}(\sqrt{\epsilon_1} + (k\epsilon_2)^{1/q} \sqrt{k\mu^2} + \sqrt{2k\theta}) \sqrt{\log(1/\epsilon)} + \frac{2k}{N} \|\Phi\|^2 < e^{-1/4} \delta$$

is equivalent to (21). This is shown by substituting ϵ_1 and ϵ_2 with their definitions, and μ and θ with their bounds in statement of the theorem. Thus, $P_{R_k}(\|RHR^*\| \geq \delta) \leq \epsilon$, which establishes the StRIP property of Φ . ■

5. EXAMPLES AND EXTENSIONS

5.1. Examples of sampling matrices. It is known [27] that experimental performance of many known RIP sampling matrices in sparse recovery is far better than predicted by the theoretical estimates. Theorems 4.1 and 4.7 provide some insight into the reasons for such behavior. As an example, take binary matrices constructed from the Delsarte-Goethals codes [39, p.461]. The parameters of the matrices are as follows:

$$(29) \quad m = 2^{2s+2}, \quad N = 2^{-r} m^{r+2}, \quad \mu = 2^r m^{-1/2}$$

where $s \geq 0$ is any integer, and where for a fixed s , the parameter r can be any number in $\{0, 1, \dots, s-1\}$. If we take s to be an odd integer and set $r = (s+1)/2$, then we obtain,

$$m = 2^{4r}, \quad N = 2^{4r^2+7r}, \quad \mu = m^{-1/4}.$$

The matrix Φ is coherence-invariant, so we put $\theta = \bar{\mu}^2$. Lemma 5.3 below implies that

$$(30) \quad \bar{\mu}^2 = \frac{N-m}{m(N-1)} < \frac{1}{m},$$

and the norm of the sampling matrix satisfies $\|\Phi\| = \sqrt{N/m}$. Thus for μ and $\bar{\mu}^2$ to satisfy the assumptions in Theorems 4.1 and 4.7, we only need m , N , and k to satisfy the relation $m = \Theta(k \log^3 \frac{N}{\epsilon})$ which is nearly optimal. Similar logic leads to derivations of such relations for other matrices. We summarize these arguments in the next proposition, which shows that matrices with nearly optimal sketch length support high-probability recovery of sparse signals chosen from the generic signal model.

Proposition 5.1. *Let Φ be an $m \times N$ sampling matrix. Suppose that it has coherence parameter $\mu = O(m^{-1/4})$ and $\theta = O(m^{-1})$, where $\theta = \bar{\mu}^2$ or $\theta = \bar{\mu}_{\max}^2$ according as Φ is coherence-invariant or not, and*

$$\|\Phi\| = O(\sqrt{N/k}).$$

If $m = \Theta(k(\log(N/\epsilon))^3)$, then Φ supports sparse recovery under Basis Pursuit for all but an ϵ proportion of k -sparse signals chosen from the generic random signal model S_k

We remark that the conditions on (mean or maximum) square coherence are generally easy to achieve. As seen from Table 1 below, they are satisfied by most examples considered in the existing literature, including both random and deterministic constructions. The most problematic quantity is the coherence parameter μ . It might either be large itself, or have a large theoretical bound. Compared to earlier work, our results rely on a more relaxed condition on μ , enabling us to establish near-optimality for new classes of matrices. For readers' convenience, we summarize in Table 1 a list of such optimal matrices along with several of their useful properties. A systematic description of all but the last two classes of matrices can be found in [4]. Therefore we limit ourselves to giving definitions and performing some not immediately obvious calculations of the newly defined parameter, the mean square coherence.

Normalized Gaussian Frames. A normalized Gaussian frame is obtained by normalizing each column of a Gaussian matrix with independent, Gaussian-distributed entries that have zero mean and unit variance. The mutual coherence and spectral norm of such matrices were characterized in [4] (see Table 1). These results together with the relation $\bar{\mu}_{\max}^2 < \mu^2$ lead to a trivial upper bound on $\bar{\mu}_{\max}^2$, namely $\bar{\mu}_{\max}^2 \leq 15 \log N/m$. Since this bound is already tight

enough for $\bar{\mu}_{\max}^2$ to satisfy the assumption of Proposition 5.1, and to avoid distraction from the main goals of the paper, we made no attempt to refine it here.

Random Harmonic Frames: Let \mathcal{F} be an $N \times N$ discrete Fourier transform matrix, i.e., $\mathcal{F}_{j,k} = \frac{1}{\sqrt{N}} e^{2\pi i j k / N}$. Let $\eta_i, i = 1, \dots, N$, be a sequence of independent Bernoulli random variables with mean $\frac{m}{N}$. Set $\mathcal{M} = \{i : \eta_i = 1\}$ and use $\mathcal{F}_{\mathcal{M}}$ to denote the submatrix of \mathcal{F} whose row indices lies in \mathcal{M} . Then the random matrix $\sqrt{\frac{|\mathcal{M}|}{N}} \mathcal{F}_{\mathcal{M}}$ is called a random harmonic frame [21, 18]. In the next proposition we compute the mean square coherence for all realizations of this matrix.

Proposition 5.2. *All instances of the random harmonic frames are coherence invariant with the following mean square coherence*

$$\bar{\mu}^2 = \frac{N - |\mathcal{M}|}{(N - 1)|\mathcal{M}|}.$$

Proof: For each $t \in [|\mathcal{M}|]$, let a_t with be the t -th member of \mathcal{M} . To prove coherence invariance, we only need to show that $\{\mu_{j,k} : k \in [N] \setminus j\} = \{\mu_{N,k} : k \in [N - 1]\}$ holds for all $j \in [N]$. This is true since

$$\mu_{j,k} = \frac{1}{|\mathcal{M}|} \sum_{t=1}^{|\mathcal{M}|} e^{\frac{2\pi i (j-k)a_t}{N}} = \mu_{N, (k-j+N) \bmod N} \quad \text{for all } k \neq j.$$

In words, the k th coherence in the set $\{\mu_{j,k}, k \in [N] \setminus j\}$ is exactly the $(k - j + N \bmod N)$ -th coherence in $\{\mu_{N,k}, k \in [N - 1]\}$, therefore the two sets are equal. We proceed to calculate the mean square coherence,

$$\begin{aligned} \bar{\mu}^2 &= \frac{1}{N(N-1)|\mathcal{M}|^2} \sum_{j \neq k, j, k=1}^N \left| \sum_{t=1}^{|\mathcal{M}|} e^{2\pi i (j-k)a_t / N} \right|^2 \\ &= \frac{1}{N(N-1)|\mathcal{M}|^2} \sum_{j \neq k, j, k=1}^N \sum_{t_1, t_2=1}^{|\mathcal{M}|} e^{2\pi i (j-k)(a_{t_1} - a_{t_2}) / N} \\ &= \frac{1}{N(N-1)|\mathcal{M}|^2} \left(\sum_{j \neq k, j, k=1}^N \sum_{t_1=t_2=1}^{|\mathcal{M}|} 1 + \sum_{t_1 \neq t_2, t_1, t_2=1}^{|\mathcal{M}|} \sum_{k=1}^N \sum_{j \neq k} e^{2\pi i (j-k)(a_{t_1} - a_{t_2}) / N} \right) \\ &= \frac{1}{N(N-1)|\mathcal{M}|^2} (N(N-1)|\mathcal{M}| - |\mathcal{M}|(|\mathcal{M}| - 1)N) \\ &= \frac{N - |\mathcal{M}|}{(N-1)|\mathcal{M}|}. \end{aligned} \quad \blacksquare$$

Chirp Matrices: Let m be a prime. An $m \times m^2$ “chirp matrix” Φ is defined by $\Phi_{t, am+b} = \frac{1}{\sqrt{m}} e^{2\pi i (bt^2 + at)/m}$ for $t, a, b = 1, \dots, m$. The coherence between each pairs of column vectors is known to be

$$\mu_{jk} = \frac{1}{\sqrt{m}} \quad (j \neq k),$$

from which we immediately obtain the inequalities $\mu \leq 1/\sqrt{m}$ and $\bar{\mu}^2 \leq 1/m$. More details on these frames are given, e.g., in [9, 22].

Equiangular tight frames (ETFs): A matrix Φ is called an ETF if its columns $\{\phi_i \in \mathbb{R}^m, i = 1, \dots, N\}$ satisfy the following two conditions:

- $\|\phi_i\|_2 = 1$, for $i = 1, \dots, N$.
- $\mu_{ij} = \sqrt{\frac{N-m}{m(N-1)}}$, for $i \neq j$.

From this definition we obtain $\mu = \sqrt{\frac{N-m}{m(N-1)}}$ and $\theta = \bar{\mu}^2 = \frac{N-m}{m(N-1)}$. The entry in the table also covers the recent construction of ETFs from Steiner systems [28].

Reed-Muller matrices: In Table 1 we list two tight frames obtained from binary codes. The Reed-Muller matrices are obtained from certain special subcodes of the second-order Reed-Muller codes [39]; their coherence parameter μ

Name	\mathbb{R}/\mathbb{C}	Coherence-Invariant	Dimensions	μ	$\theta(\Phi)$
Normalized Gaussian (G)	\mathbb{R}	No	$m \times N$	$\leq \frac{\sqrt{15 \log N}}{\sqrt{m} - \sqrt{12 \log N}}$	$\leq \mu^2$
Random harmonic (RH)	\mathbb{C}	Yes	$ \mathcal{M} \times N, \frac{1}{2}m \leq \mathcal{M} \leq \frac{3}{2}m$	$\leq \sqrt{\frac{118(N-m) \log N}{mN}}$	$\leq \frac{N- \mathcal{M} }{ \mathcal{M} (N-1)}$
Chirp (C)	\mathbb{C}	Yes	$m \times m^2$	$\frac{1}{\sqrt{m}}$	$\frac{1}{m+1}$
ETF (including Steiner)	\mathbb{C}	Yes	$\sqrt{N} \leq m \leq N$	$\sqrt{\frac{N-m}{m(N-1)}}$	μ^2
Reed-Muller (RM)	\mathbb{R}	Yes	$2^s \times 2^{t(1+s)}$	$\leq \frac{1}{\sqrt{2^{2s-2t-1}}}$	$\leq 2^{-s}$
Delsarte-Goethals set (DG)	\mathbb{R}	Yes	$2^{2s+2} \times 2^{2(s+1)(r+2)-r}$	2^{r-s-1}	$\leq 2^{-2s-2}$
Deterministic subFourier (SF)	\mathbb{C}	Yes	$m \times p$	$e^{3d} m^{-1/(9d^2 \log d)}$	$\leq \frac{1}{m}$

Name	$\ \Phi\ $	Restrictions	Probability	Sketch dimensions: $m = \Omega(\cdot)$
G	$\leq \frac{\sqrt{m} + \sqrt{N} + \sqrt{2 \log N}}{\sqrt{m} - \sqrt{8m \log N}}$	$60 \log N \leq m \leq \frac{N-1}{4 \log N}$	$\geq 1 - \frac{11}{N}$	$k \log^2 N$
RH	$\leq \frac{2N}{m}$	$16 \log N \leq m \leq \frac{N}{3}$	$\geq 1 - \frac{4}{N} - \frac{1}{N^2}$	$k \log^2 N$
C	\sqrt{m}	m is prime	deterministic	$k \log m$
ETF	$\sqrt{\frac{N}{m}}$	$\sqrt{\frac{M(N-1)}{N-M}}, \sqrt{\frac{(N-m)(N-1)}{m}}$ are odd integers	deterministic	$k \log m$
RM	$2^{ts/2}$	$t < s/4$	deterministic	$k \log^3 N$
DG	$2^{(s+1)(r+1)-r/2}$	$r < s/2$	deterministic	$k \log^3 N$
SF	$\sqrt{p/m}$	p is prime, $p^{1/(d-1)} \leq m \leq p$	deterministic	$(k \log^2 N) \frac{9d^2 \log d}{4}$

TABLE 1. Examples for Prop. 5.1: Classes of sampling matrices satisfying the incoherence conditions

is found in [4] and the mean square coherence is found from (30). The Delsarte-Goethals matrices are also based on some subcodes of the second order Reed-Muller codes and were discussed earlier in this section. Both dictionaries support orthogonal arrays, and therefore, form unit-norm tight frames (rows of the matrix Φ are pairwise orthogonal), with a consequence that $\|\Phi\| = \sqrt{N/m}$. We include these two examples out of many other possibilities based on codes because they appear in earlier works, and because their parameters are in the range that fits well our conditions.

We note that the quaternary version of these frames is also of interest in the context of sparse recovery; see in particular [12].

Deterministic Fourier Construction[31]: Let $p > 2$ be a prime, and let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree $d > 2$ over the finite field \mathbb{F}_p . Suppose that m is some integer satisfying $p^{1/(d-1)} \leq m \leq p$. Then we can construct an $m \times p$ deterministic RIP matrix from a $p \times p$ DFT matrix by keeping only the rows with indices in $\{f(n) \pmod{p}, n = 1, \dots, m\}$, and normalizing the columns of the resulting matrix. It is known that this matrix has mutual coherence no greater than $e^{3d} m^{-1/(9d^2 \log d)}$. Even though this bound is an artifact of the proof technique used in [31], there seem to be no obvious ways of improving it.

5.2. StRIP matrices from orthogonal arrays. Let us briefly consider another way of constructing StRIP matrices based on elementary arguments. Let $\mathcal{C} = \{\phi_1, \dots, \phi_N\}$ be a collection of binary m -vectors. We assume that the entries of the vectors are of the form $\pm 1/\sqrt{m}$ and denote the correlation of ϕ_i and ϕ_j by $\mu_{ij} = |\langle \phi_i, \phi_j \rangle|$.

The set \mathcal{C} is called an orthogonal array of strength t if every subset of $r \leq t$ coordinates of the vectors of \mathcal{C} supports a uniformly random binary r -vector. A good reference for orthogonal arrays is the book by Hedayat et al. [32]. An orthogonal array has the property that any t coordinates of a randomly chosen vector behave as independent random variables (therefore, of course, t is much smaller than m). In particular, the first t moments of the distance distribution of \mathcal{C} are equal to the moments of the binomial distribution. Let $d_{ij} = \frac{m}{2}(1 - \phi_i^T \phi_j)$ be the Hamming distance between ϕ_i and ϕ_j .

Lemma 5.3. (Pless identities, e.g. [39, p.132]) *Let \mathcal{C} be an orthogonal array of strength t . Let $B_w = (1/N)|\{(\phi_i, \phi_j) \in \mathcal{C}^2 \mid d_{ij} = w\}|$ be the number of pairs of vectors in \mathcal{C} at distance w . For all $l = 1, 2, \dots, t$*

$$(31) \quad \sum_{w=0}^m \frac{B_w}{N} \left(w - \frac{m}{2}\right)^l = \frac{1}{2^m} \sum_{w=0}^m \binom{m}{w} \left(w - \frac{m}{2}\right)^l.$$

We will need a manageable estimate of the right-hand side of (31). We quote from [39, p.288]: let $l \geq 2$ be even, then

$$(32) \quad \frac{1}{2^m} \sum_{w=0}^m \binom{m}{w} \left(w - \frac{m}{2}\right)^l \leq \left(\frac{ml}{4e}\right)^{l/2} \sqrt{l} e^{1/6}.$$

The main result of this section is given by the following theorem.

Theorem 5.4. *Let \mathcal{C} be an orthogonal array of strength t and cardinality N and let $l \leq t$ be even. If $m \geq (3/4)l(k/\delta)^2(k/\epsilon)^{2/l}$ then Φ is (k, δ, ϵ) -StRIP.*

Proof. Let $I \subset [N]$ be a uniformly random k -subset. We clearly have

$$\lambda_{\min}(\Phi_I^T \Phi_I) \|\mathbf{x}\|_2^2 \leq \|\Phi_I \mathbf{x}\|_2^2 \leq \lambda_{\max}(\Phi_I^T \Phi_I) \|\mathbf{x}\|_2^2,$$

where $\lambda_{\min}(\cdot)$ and $\lambda_{\max}(\cdot)$ are the minimum and maximum eigenvalues of the argument.

By the Gershgorin theorem, any eigenvalue λ of the Gram matrix $\Phi_I^T \Phi$ satisfies

$$|\lambda - 1| \leq \sum_{j \in I_i} \mu_{ij},$$

for some $i \in [N]$, where we used the notation $I_i := I \setminus \{i\}$. Now consider the probability that for some $i \in I$ the sum $\sum_{j \in I_i} \mu_{ij} > \delta$. The proof will be finished if we show that this probability is less than ϵ . Let $I = \{i_1, \dots, i_k\}$. We have

$$\begin{aligned} P_{R_k}(\exists i \in I : \sum_{j \in I_i} \mu_{ij} > \delta) &\leq k P_{R_k}\left(\sum_{j \in I_{i_1}} \mu_{i_1, j} > \delta\right) \leq k \frac{1}{\delta^l} \mathbb{E}_{R_k} \left(\sum_{j \in I_{i_1}} \mu_{i_1, j}\right)^l \\ &= k \frac{(k-1)^l}{\delta^l} \mathbb{E}_{R_k} \left(\frac{1}{k-1} \sum_{j \in I_{i_1}} \mu_{i_1, j}\right)^l \\ &\leq \frac{k(k-1)^{l-1}}{\delta^l} \mathbb{E}_{R_k} \sum_{j \in I_{i_1}} \mu_{i_1, j}^l, \end{aligned}$$

where the last step uses convexity of the function $z \mapsto z^l$. The trick is to show that the expectation on the last line, presently computed over the choice of I , can be also found with respect to a pair of random uniform elements of \mathcal{C} chosen without replacement. This is established in the next calculation:

$$\begin{aligned} \mathbb{E}_{R_k} \sum_{j \in I_{i_1}} \mu_{i_1, j}^l &= \sum_{i_1 < i_2 < \dots < i_k} \frac{1}{\binom{N}{k}} \sum_{j=2}^k \mu_{i_1, i_j}^l = \frac{1}{k! \binom{N}{k}} \sum_{i_1 \neq i_2 \neq \dots \neq i_k} \sum_{j=2}^k \mu_{i_1, i_j}^l \\ &= \frac{1}{N(N-1)} \sum_{j=2}^k \sum_{i_1=1}^N \sum_{i_j \neq i_1} \mu_{i_1, i_j}^l \\ (33) \quad &= (k-1) \mathbb{E} \mu_{ij}^l, \end{aligned}$$

where the expectation on the last line (and below in the proof) is computed with respect to a pair of uniformly chosen distinct random vectors from \mathcal{C} . Next using (31) and switching to the variable $w = (m/2)(1 - \mu)$, we obtain

$$\begin{aligned} \mathbb{E} \mu_{ij}^l &= \left(\frac{2}{m}\right)^l \sum_{w=1}^m \frac{B_w}{N-1} \left(w - \frac{m}{2}\right)^l \\ &= \left(\frac{2}{m}\right)^l \frac{N}{N-1} \left[\sum_{w=0}^m \frac{B_w}{N} \left(w - \frac{m}{2}\right)^l - \frac{1}{N} \left(\frac{m}{2}\right)^l \right] \\ &= \left(\frac{2}{m}\right)^l \frac{N}{N-1} \left[\frac{1}{2^m} \sum_{w=0}^m \binom{m}{w} \left(w - \frac{m}{2}\right)^l - \frac{1}{N} \left(\frac{m}{2}\right)^l \right], \end{aligned}$$

Now we can use (32) and $l < m$ to write

$$\mathbb{E} \mu_{ij}^l \leq \left(\frac{l}{em}\right)^{l/2} \frac{N}{N-1} \sqrt{le^{1/3}} - \frac{1}{N-1} \leq e^{1/6} l^{(l+1)/2} (em)^{-l/2}.$$

Conclude using the condition on m :

$$P_{R_k} \left(\exists i \in I : \sum_{j \in I_i} \mu_{ij} > \delta \right) \leq k^{l+1} \delta^{-l} e^{1/6} l^{(l+1)/2} (em)^{-l/2} < \epsilon.$$

Observe that the condition of this theorem is nonasymptotic, and is satisfied by a number of known constructions of orthogonal arrays. ■

Example: Consider sampling matrices obtained from the binary Delsarte-Goethals codes already mentioned above; see Eq.(29). It is known that the underlying code forms an orthogonal array of strength $t = 7$, so taking $l = 6$ we obtain a family of (k, δ, ϵ) -StRIP matrices of dimensions $m \times N$ for sparsity

$$k \leq 0.52 (\delta^6 \epsilon m^3)^{1/7} = 0.52 (\delta^6 \epsilon)^{1/7} (2^r N)^{3/(7(r+2))}.$$

The case $r = 0$ was considered in [13] where these matrices were analyzed based on the detailed properties of this particular case of the construction. Our computation, while somewhat crude, permits a uniform estimate for the entire family of matrices. The estimate can be improved if the expectation $\mathbb{E} \mu_{ij}^l$ can be computed explicitly from the known distribution of correlations. For instance, taking $r = 1$ and using the distribution given in [39, p.477] we obtain that $\mathbb{E} \mu^6 \approx (4/3)m^{-3}$. With this, the condition on sparsity that emerges has the form $k < 0.95 (\delta^6 \epsilon m^3)^{1/7}$, with a better constant compared to the general estimate. For instance, we obtain $m \times (m^3/2)$ matrices with the $(k, \delta, 0.001)$ StRIP property for all $k \leq 0.35 \delta^{6/7} m^{3/7}$.

Another similar possibility arises if \mathcal{C} is taken to be a binary dual BCH code with $m = 2^s - 1$, $N = m^r$, $\mu = 2(r-1)m^{-1/2}$, $r = 1, 2, 3, \dots$. Many more such constructions can be obtained from other algebraic codes such as the Kerdock codes, Gold codes, etc. [33]. This lends further support to earlier studies of sampling matrices constructed from the BCH codes [1], Delsarte-Goethals codes, and other binary codes related to the second-order Reed-Muller codes [12, 13].

It would be desirable to show that orthogonal arrays also suffice for the SINC property; however, the technique introduced above results in parameters that contradict the Rao bound on the number of rows in an array [32]. Thus, we are unable to show that this construction results in matrices that are good for linear estimators.

5.3. Further constructions from binary codes. We remark that it is easy to show existence of matrices with low coherence. The following observation is a rephrasing of the result known in coding theory as the Gilbert-Varshamov existence bound for binary linear codes.

Proposition 5.5. *Let $l = \log_2 N$, $l < m$ and let $G = (g_1, \dots, g_l)$ be an $m \times l$ binary matrix whose rows are chosen independently and uniformly from \mathbb{F}_2^l . Let $m = 4 \log N / \mu^2$, where $0 < \mu < 1$. Form the matrix Φ by constructing an \mathbb{F}_2 -linear span of the columns of G and using the map $\{0, 1\} \rightarrow \{\frac{1}{\sqrt{m}}, \frac{-1}{\sqrt{m}}\}$. Then Φ has coherence μ with probability at least $1 - 2/N$ and mean square coherence $\bar{\mu}^2 < 1/m$ with probability at least $(1 - (m/N))^m$.*

Proof. Note that the Hamming distance d between any two columns of a matrix with coherence μ satisfies $\mu \geq |1 - 2d/m|$. The set of columns of C forms a linear space, so it suffices to argue about Hamming weights rather than pairwise correlations. Let $\mathbf{u} \in \{0, 1\}^l$ be a nonzero vector, then the probability that the vector $\mathbf{v} = G\mathbf{u}$ has weight w equals $\binom{m}{w} 2^{-m}$. Let X be the random number of columns with weight $|w - m/2| \geq m\mu/2$. We have

$$(34) \quad \mathbb{E} X \leq 2 \frac{N-1}{2^m} \sum_{w=0}^{m(\frac{1}{2}-\frac{\mu}{2})} \binom{m}{w} \leq N 2^{1-m(1-h(\frac{1}{2}-\frac{\mu}{2}))}$$

where $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy function. Using the inequality

$$1 - h(1/2 - x) \geq 2x^2 / \log 2, \quad 0 \leq x < 1/2$$

and the condition for μ , we obtain $\mathbb{E} X \leq 2/N$. Since $P(X > 0) \leq \mathbb{E} X$, this implies the first claim. The second part follows because there are $\prod_{i=1}^m (N - i)$ matrices G with distinct nonzero rows. ■

The derandomizing of Gilbert-Varshamov codes was recently addressed by Porat and Rothschild [43]. They presented a $O(mN)$ deterministic algorithm that constructs codes with large minimum distance. To construct incoherent dictionaries, we need a bit more, namely that all the pairwise distances are in a narrow segment around $m/2$. The algorithm in [43] can be easily tailored to do this. A simplified version of this procedure which results in the algorithm of complexity $O(mN^2)$ (i.e., not as good as in [43]), was given in [40]. In a nutshell it is as follows. Instead of

constructing the $m \times N$ matrix, $N = 2^l$, we aim at constructing a basis of the space of columns, i.e., an $m \times l$ matrix G . The rows of G are selected recursively. Before any rows are selected, the expected number of codewords of weight far from $m/2$ is given by (34). The algorithm selects rows one by one so that the expectation of the number of outlying vectors *conditional* on the rows already chosen is the smallest possible.

We note that in the context of sparse recovery, the dependence between N and m is likely to be polynomial. In this range of parameters the above complexity is acceptable and is in fact comparable with the size of the matrix Φ which needs to be stored for sampling and processing.

REFERENCES

- [1] N. Ailon and E. Liberty, *Fast dimension reduction using Rademacher series on dual BCH codes*, Discrete Comput. Geom. **42** (2009), no. 4, 615–630.
- [2] N. Alon, O. Goldreich, J. Høstad, and R. Peralta, *Simple constructions of almost k -wise independent random variables*, Random Structures and Algorithms **3** (1992), 289–304.
- [3] W. U. Bajwa, R. Calderbank, and S. Jafarpour, *Why Gabor frames? Two fundamental measures of coherence and their role in model selection*, J. Commun. Networks **12** (2010), 289–307.
- [4] W. U. Bajwa, R. Calderbank, and D. G. Mixon, *Two are better than one: fundamental parameters of frame coherence*, Appl. Comput. Harmon. Anal. **33** (2012), no. 1, 58–78.
- [5] A. S. Bandeira, M. Fickus, D. G. Mixon, and P. Wong, *The road to deterministic matrices with the restricted isometry property*, arXiv:1202.1234.
- [6] A. Barg and A. Mazumdar, *Small ensembles of sampling matrices constructed from coding theory*, Proc. IEEE International Symposium on Information Theory, Austin, TX, June 2010, pp. 1963–1967.
- [7] A. Ben-Aroya and A. Ta-Shma, *Constructing small-bias sets from algebraic-geometric codes*, 2009 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), IEEE Computer Soc., Los Alamitos, CA, 2009, pp. 191–197.
- [8] J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova, *Explicit constructions of RIP matrices and related problems*, arXiv:1008.4535.
- [9] A. Brodzik, *On the fourier transform of finite chirps*, IEEE Signal Processing Letters **13** (2006), 541–544.
- [10] A. M. Bruckstein, D. L. Donoho, and M. Elad, *From sparse solutions of systems of equations to sparse modeling of signals and images*, SIAM Review **51** (2009), no. 1, 34–81.
- [11] T. T. Cai, G. Xu, and J. Zhang, *On recovery of sparse signals via ℓ_1 minimization*, IEEE Trans. Inform. Theory **55** (2009), no. 1, 3388–3397.
- [12] R. Calderbank, S. Howard, and S. Jafarpour, *Construction of a large class of deterministic sensing matrices that satisfy a statistical restricted isometry property*, IEEE J. Selected Topics Signal Proc. **4** (2010), no. 2, 358–374.
- [13] R. Calderbank and S. Jafarpour, *Reed-Muller sensing matrices and the LASSO*, Sequences and Their Applications (SETA2010), Lect. Notes Comput. Science, vol. 6338 (C. Carlet and A. Pott, eds.), 2010, pp. 442–463.
- [14] E. J. Candès, *The restricted isometry property and its implications for compressed sensing*, C. R. Math. Acad. Sci. Paris **346** (2008), no. 9–10, 589–592.
- [15] E. J. Candès and Y. Plan, *Near-ideal model selection by ℓ_1 minimization*, Ann. Statist. **37** (2009), no. 5A, 2145–2177.
- [16] E. J. Candès and Y. Plan, *A probabilistic and RIPless theory of compressed sensing*, IEEE Trans. Inform. Theory **57** (2011), no. 11, 7235–7254.
- [17] E. J. Candès and J. Romberg, *Sparsity and incoherence in compressive sampling*, Inverse Problems **23** (2007), 969–985.
- [18] E. J. Candès, J. Romberg, and T. Tao, *Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 489–509.
- [19] E. J. Candès, J. K. Romberg, and T. Tao, *Stable signal recovery from incomplete and inaccurate measurements*, Comm. Pure Appl. Math. **59** (2006), no. 8, 1207–1223.
- [20] E. J. Candès and T. Tao, *Decoding by linear programming*, IEEE Trans. Inform. Theory **51** (2005), no. 12, 4203–4215.
- [21] ———, *Near-optimal signal recovery from random projections: universal encoding strategies?*, IEEE Trans. Inform. Theory **52** (2006), no. 12, 5406–5425.
- [22] P. Casazza and M. Fickus, *Fourier transforms of finite chirps*, EURASIP J. Appl. Signal Processing (2006), 1–7, Article ID 70204.
- [23] S. S. Chen, D. L. Donoho, and M. A. Saunders, *Atomic decomposition by basis pursuit*, SIAM J. Sci. Comput. **20** (1998), no. 1, 33–61.
- [24] W. Dai and O. Milenkovic, *Weighted superimposed codes and constrained integer compressed sensing*, IEEE Trans. Inform. Theory **55** (2009), no. 5, 2215–2229.
- [25] R. A. DeVore, *Deterministic constructions of compressed sensing matrices*, J. Complexity **23** (2007), no. 4–6, 918–925.
- [26] D. L. Donoho and M. Elad, *Optimally sparse representations in general (nonorthogonal) dictionaries via ℓ^1 minimization*, Proc. Natl. Acad. Sci. **100** (2003), 2197–2202.
- [27] D. L. Donoho and J. Tanner, *Observed universality of phase transitions in high-dimensional geometry, with implications for modern data analysis and signal processing*, Phil. Trans. Royal Soc. **367** (2009), 4273–4293.
- [28] M. Fickus, D. G. Mixon, and J. C. Tremain, *Steiner equiangular tight frames*, Linear Algebra Appl. **436** (2012), no. 5, 1014–1027.
- [29] J.-J. Fuchs, *On sparse representations in arbitrary redundant bases*, IEEE Trans. Inform. Theory **50** (2004), no. 6, 1341–1344.
- [30] A. Gurevich and R. Hadani, *Statistical RIP and semi-circle distribution of incoherent dictionaries*, 2009, arXiv:0903.3627.
- [31] J. Haupt, L. Applebaum, and R. Nowak, *On the restricted isometry of deterministically subsampled Fourier matrices*, Proc. 44th Annual Conf. Information Sciences and Systems (CISS), 2010, pp. 1–6.
- [32] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal arrays*, Springer-Verlag, New York, 1999.
- [33] T. Helleseth and P. V. Kumar, *Sequences with low correlation*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), vol. II, Elsevier Science, 1998, pp. 1768–1853.

- [34] A. Juditsky and A. Nemirovski, *Accuracy guarantees for ℓ_1 -recovery*, IEEE Trans. Inform. Theory **57** (2010), no. 12, 7818–7839.
- [35] ———, *On verifiable sufficient conditions for sparse signal recovery via ℓ_1 minimization*, Math. Program. Ser. B **127** (2011), 57–88.
- [36] B. S. Kashin and V. N. Temlyakov, *A remark on the problem of compressed sensing*, Math. Notes **82** (2007), no. 5-6, 748–755.
- [37] D. B. Khanh, P. Indyk, E. Price, and D. P. Woodruff, *Lower bounds for sparse recovery*, Proc. 21st Annual ACM-SIAM Sympos. Discrete Algorithms (SODA '10), 2010, pp. 1190–1197.
- [38] M. Ledoux and M. Talagrand, *Probability in Banach spaces: Isoperimetry and processes*, Springer, 1991.
- [39] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1991.
- [40] A. Mazumdar, *Combinatorial methods in coding theory*, Ph.D. thesis, University of Maryland, 2011, <http://hdl.handle.net/1903/11547>.
- [41] C. McDiarmid, *On the method of bounded differences*, Surveys in combinatorics, 1989 (Norwich, 1989), London Math. Soc. Lecture Note Ser., vol. 141, Cambridge Univ. Press, Cambridge, 1989, pp. 148–188.
- [42] J. L. Nelson and V. N. Temlyakov, *On the size of incoherent systems*, Journ. Approx. Theory **163** (2011), 1238–1245.
- [43] E. Porat and A. Rothschild, *Explicit non-adaptive combinatorial group testing schemes*, Automata, languages and programming. Part I, Lecture Notes in Comput. Sci., vol. 5125, Springer, Berlin, 2008, pp. 748–759.
- [44] M. Rudelson and R. Vershynin, *Sampling from large matrices: An approach through geometric functional analysis*, J. Assoc. Comput. Mach. **54** (2007), no. 4, 1–19.
- [45] R. Tibshirani, *Regression shrinkage and selection via the lasso*, J. Roy. Statist. Soc. Ser. B **58** (1996), 267–288.
- [46] J. A. Tropp, *Greed is good: Algorithmic results for sparse approximation*, IEEE Trans. Inform. Theory **50** (2004), no. 10, 2231–2242.
- [47] ———, *Recovery of short, complex linear combinations via ℓ_1 minimization*, IEEE Trans. Inform. Theory **51** (2005), no. 4, 1568–1570.
- [48] ———, *Norms of random submatrices and sparse approximation*, C.R. Acad. Sci. Paris, Ser. I **346** (2008), 1271–1274.
- [49] ———, *On the conditioning of random subdictionaries*, Appl. Comput. Harmon. Anal. **25** (2008), no. 1, 1–24.